Hochschule Hannover

University of Applied Sciences and Arts

Fakultät I – Elektro und Informationstechnik

Fachgebiet: Automatisierungstechnik und Prozessinformatik

Bachelorarbeit

Thema

„Entwicklung eines Leitfadens für die Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen“

eingereicht von:

Name: Marian Thöne

Matrikelnummer: 1551261

Zeitraum:

von: 01.04.2023

bis: 03.07.2023

Erstprüfer: Prof. Dr.-Ing. Karl-Heinz Niemann

Zweitprüfer: M. Eng. Jan-Niklas Puls

I Selbstständigkeitserklärung und Lizenzinformationen

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, sind als solche gekennzeichnet. Ich habe die Arbeit in gleicher oder ähnlicher Form bei keiner anderen Prüfungsbehörde vorgelegt.

Celle, den 03.07.2023

Unterschrift aus
Datenschutzgründen entfernt.

_____

Unterschrift (Marian Thöne)

https://doi.org/10.25968/opus-2980

II Versionshistorie

Version	Datum	Bemerkung	Erstellende Person
1.0	02.07.2023	Erstausgabe	MarTh
1.1	31.07.2023	Korrigierte Erstausgabe – Kommentare von Erst- und Zweitprüfer – Hinzufügen der „CC BY 4.0“ Lizenz	MarTh
2.0	23.10.2023	Zweitausgabe – Hinzufügen der DOI	MarTh

III Vorwort

In der vorliegenden Arbeit wird ein Leitfaden zur Einrichtung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen (KMU) entwickelt. Ein Informationssicherheitsmanagementsystem (ISMS) ist im Grunde eine geordnete Ansammlung an Verfahren, Regeln und Maßnahmen zur Wahrung der Sicherheit von Informationen. Mit diesem System wird die Steuerung und Kontrolle der Informationssicherheit durch strukturierte Vorgehensweisen entscheidend verbessert.

In dieser Bachelorarbeit werden in den ersten Kapiteln die relevanten Normen und Richtlinien (insbesondere aus der DIN EN ISO/IEC 27000 Normenfamilie und aus den Richtlinien der VdS 10000 sowie VdS 10005) betrachtet. Auf dieser Grundlage wird in den darauffolgenden Kapiteln der grundlegende Aufbau eines ISMS für Unternehmen erklärt. Im Anschluss wird diese Thematik auf KMU übertragen. Im weiteren Verlauf wird die Entwicklung des Leitfadens beschrieben, wobei auch auf den allgemeinen Aufbau eines Leitfadens eingegangen wird. Der eigentliche Leitfaden ist in Anhang A dieses Dokumentes zu finden. Der Leitfaden kann losgelöst von dieser Arbeit eingesetzt werden.

„Angesichts des Fachkräftemangels müssen wir in das Know-how der kleinen und mittelständischen Unternehmen investieren, damit sie sich ausreichend vor Cyberangriffen schützen können.“

Johannes Bussmann (Präsident des TÜV-Verbandes) [1]

Prolog

In this thesis, a guideline for the establishment of an information security management system in small and medium-sized enterprises (SMEs) is developed. An information security management system (ISMS) is basically an ordered collection of procedures, rules and measures to maintain the security of information. With this system, the management and control of information security is decisively improved through structured procedures.

In this bachelor thesis, the relevant standards and guidelines (in particular from the DIN EN ISO/IEC 27000 family of standards and from the VdS 10000 and VdS 10005 guidelines) are considered in the first chapters. On this basis, the basic structure of an ISMS for companies is explained in the following chapters. Subsequently, this topic is transferred to SMEs. In the further course, the development of the guideline is described, whereby the general structure of a guideline is also dealt with. The actual guide can be found in Appendix A of this document. The guide can be used separately from this paper.

„In view of the shortage of skilled workers, we must invest in the know-how of small and medium-sized enterprises so that they can adequately protect themselves against cyber-attacks.“

Johannes Bussmann (President of the TÜV Association) [1] (translated by deepl.com)

IV Inhaltsverzeichnis

V Glossar/Abkürzungsverzeichnis

Deutsch	**Beschreibung**
Asset	Ein Asset ist ein Vermögensgegenstand oder ein aktiver Wert, der schützenswert ist [2]. Im sog. Asset-Inventar werden alle Assets unabhängig des Wertes aufgelistet [3]. Diese Auflistung ist essentiell wichtig für eine erfolgreiche und schnelle Risikoanalyse. Beispiele für Assets sind Server, Maschinen, Gebäude oder Umlaufvermögen.
Bedrohung	Durch Schwachstellen ausgelöste potentielle Gefahren werden als Bedrohung angesehen. Wird z.B. der Informationsgehalt einer Nachricht ausspioniert („Man-In-The-Middle“ – Angriff) oder manipuliert, handelt es sich um eine Bedrohung für die beiden Kommunikationspartner. Bedrohungen können darüber hinaus von der Technik (z.B. Kabelbrand), durch eine Fehlbedienung eines Mitarbeitenden (z.B. Überfahren eines Stop-Signals) oder durch das Anwenden von Gewalt ausgehen.
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
Cyberangriff	Von außen (durch einen einzelnen Hacker, durch eine Institution o. ä.) zum Zweck der Sabotage oder der Informationsgewinnung geführter Angriff auf ein Computernetzwerk [4–6]
DIN	**D**eutsches **I**nstitut für **N**ormung
EN	**E**uropäische **N**orm
Echtzeitschutz	Ein Echtzeitschutz überwacht das System permanent in Echtzeit und schützt jederzeit vor Infektionen. Er läuft automatisch im Hintergrund und überwacht das System kontinuierlich vgl. [7].
IEC	Internationale Elektrotechnische Kommission (**I**nternational **E**lectrotechnical **C**ommission)
ISB	**I**nformations**s**icherheits**b**eauftragte(r)

ISO	Internationale Organisation für Normung (**I**nternational **O**rganization for **S**tandardization)
IST	**I**nformations**s**icherheits**t**eam
ITV	**IT**-**V**erantwortliche(r) **(I**nformations**t**echnologie**v**erantwortliche(r))
KMU	**K**leine (und sehr kleine) und **m**ittlere **U**nternehmen mit weniger als 250 Mitarbeitenden [8] • **sehr kleine** Unternehmen: weniger als **zehn** Mitarbeitende maximale Jahresbilanzsumme von **zwei** Mio. Euro • **kleine** Unternehmen: weniger als **50** Mitarbeitende maximale Jahresbilanzsumme von **zehn** Mio. Euro • **mittlere** Unternehmen: weniger als **250** Mitarbeitende maximale Jahresbilanzsumme von **43** Millionen Euro
KRITIS	Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. [9] (Bspw. Klärwerke, Energieversorger, Atomkraftwerke, Chemiekonzerne)
Leitfaden	Kurze, übersichtliche und gut verständliche Handlungsanweisung mit einem leicht bindenden Charakter [10]
Geschäftsleitung	• Oberste Leitungsebene in einem Unternehmen • geschäftsführende Direktion • Inhaber(in) oder Geschäftsführung bei kleineren Unternehmen
Man-In-The-Middle - Angriff	Bei einem „Man-in-the-Middle“-Angriff schaltet sich eine fremde Partei in eine bestehende Kommunikation ein, hört diese – meist unbemerkt – ab und ist in der Lage die Daten zu manipulieren. [11]

Norm	Dokument, das Regeln, Leitlinien oder Merkmale für Tätigkeiten festlegt [12]
Richtlinie	Eine Richtlinie ist eine Handlungs- oder Ausführungsvorschrift einer Institution oder Instanz, die jedoch kein förmliches Gesetz ist. [13]
Risiko	Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit und Ausmaß eines Schadens. Als Risiko werden Szenarien beschrieben, die eine Relevanz für den vorliegenden Fall darstellen [14, S. 33]. Risiken sind das Zusammenspiel aus Assets, Schwachstellen und daraus resultierenden Bedrohungen.
Schwachstelle	Eine Schwachstelle ist eine Lücke in der Informationssicherheit. Sie stellt eine Bedrohung dar, da hierdurch Unbefugten der Zugang zu Systemressourcen und vertraulichen Daten möglich ist. Die Ursachen für die Schwachstelle können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration oder dem Betrieb sowie dem Unternehmen liegen [14, S. 33].
SME	**S**mall (and very small) and **m**edium-sized **e**nterprises with less than 250 employees [9] • **very small** enterprises: less than **ten** employees maximum annual balance sheet total of **two** million euros • **small** enterprises: less than **50** employees maximum annual balance sheet total of **ten** million euros • **medium-sized** enterprises: less than **250** employees maximum annual balance sheet total of **43** million euros (translated with the help of deepl.com)

Stakeholder/ Stakeholderinnen	Gruppe von Personen, die ein berechtigtes Interesse an der Entwicklung eines Unternehmens haben [15]
	• interne Stakeholder/Stakeholderinnen
	  ○ Mitarbeitende
	  ○ Manager/Managerinnen - Geschäftsleitung
	  ○ Eigentümer/Eigentümerinnen
	• externe Stakeholder/Stakeholderinnen
	  ○ Lieferanten/Lieferantinnen
	  ○ Kunden/Kundinnen
	  ○ Gläubiger/Gläubigerinnen

VdS	Ehemals „**V**erband **d**er **S**achversicherer“, heute 100%ige Tochter der „Deutschen Versicherungswirtschaft“ (GDV) [16]

1 Einleitung

Im ersten Kapitel dieser Arbeit erfolgt eine Einführung in das Thema und die Aufgabenstellung. Des Weiteren werden der Aufbau der vorliegenden Arbeit beschrieben, kleine und mittlere Unternehmen definiert und die Adressaten des erarbeiteten Leitfadens vorgestellt.

1.1 Einführung in das Thema

Informationstechnologien sind heutzutage aus der Wirtschaftswelt nicht mehr wegzudenken. Dabei ist in Zeiten von Cyber-Angriffen die Informationssicherheit unverzichtbar, um die Wirtschaftswelt vor Schäden zu bewahren. Gleichzeitig sollte die Informationssicherheit so ausgerichtet sein, dass die Geschäftsziele der Unternehmen optimal unterstützt werden und die Informationssicherheit nicht zum Hemmnis bei der Nutzung von Informationstechnologien wird.

Die Informationssicherheit zielt daher auf den Schutz der Informationen in einem Unternehmen ab. Früher wie heute müssen Unternehmen Ihre Betriebsgeheimnisse vor der Konkurrenz schützen (bspw. das Rezept der „Echten Sachertorte“ [17], das Ur-Coca-Cola-Rezept oder Kundendaten). Das Vorhandensein und die alleinige Verwendungsmöglichkeit dieser Informationen unter Ausschluss der Kenntnisnahme durch Dritte sind aus Sicht von Unternehmen besonders schützenswert.

Mit der Zeit kamen immer mehr schützenswerte Ideen und Informationen hinzu. Früher wurden diese z. B. mithilfe von Karteikartensystemen oder in einem Tresor vor den gierigen Augen von Wirtschaftsspionen verborgen. Heutzutage werden viele dieser Informationen auch digital gespeichert. Dies erleichtert die Verwaltung und die Speicherung der schützenswerten Informationen. Der Tresor von früher war jedoch für Angreifende ziemlich schwer zu erreichen und konnte von den zuständigen Personen relativ einfach bewacht werden. Im Zeitalter der Digitalisierung, in dem die Informationen auf großen Servern, die teilweise nicht mal mehr im eigenen Unternehmen stehen, gespeichert werden, können Wirtschaftsspione oder andere Kriminelle viel leichter (über das Internet) an diese Informationen gelangen. Hierfür und für eine ganzheitliche Betrachtung der Informationssicherheit bedarf es Verfahren und Regelungen, die den Schutz der Informationen bestmöglich gewährleisten.

Für die Umsetzung einer ganzheitlichen Sicherheitsstrategie bietet ein nach internationalen Standards aufgebautes Informationssicherheitsmanagementsystem (ISMS) eine solide Grundlage. Ein ISMS ist ein System, das die Etablierung von Informationssicherheitsprozessen und -regeln beschreibt und ein systematisches Vorgehen zur Abwehr von Cyber-Angriffen implementiert.

Dabei ist ein ISMS kein einmaliger Prozess. Vielmehr wird durch kontinuierliche Verbesserungsverfahren in einem ISMS die Informationssicherheit des Unternehmens an den fortschreitenden Stand der Technik und an neue Risiken und Bedrohungen angepasst.

Bei der Einführung eines solchen Managementsystems darf der Faktor „Mensch“ nicht außer Acht gelassen werden, da viele Nutzende darauf vertrauen, dass die Geräte, die ihnen von dem Unternehmen gestellt werden, so gebaut und programmiert sind, dass diese sie vor den Gefahren wie bspw. dem unbefugten Zugriff durch Dritte von außen schützen. Oftmals haben sie auch keine Vorstellung bzw. wenig Gefahrenbewusstsein, wie schnell und durch welche Schwachstellen Cyber-Kriminelle in das jeweilige System eindringen können. Die Kenntnis über die Bedienung der technischen Geräte reicht den Mitarbeitenden vielfach aus, um die Arbeit unter Zuhilfenahme des technischen Geräts zu erledigen, ohne sich mit dem Sicherheitsrisiko zu beschäftigen. Dieses trügerische Vertrauen in Bezug auf Informationstechnik bzw. eine nachlässige Technikeinstellung steigern die Erfolgsaussichten bei Cyberangriffen auch bei kleinen und mittleren Unternehmen (KMU).

Die Cybersicherheit von Informationstechnologien muss ein zentraler Baustein der Digitalisierung sein, um Angriffe präventiv vermeiden oder entsprechend erkennen und abwehren zu können. Die Notwendigkeit von Informationssicherheit zeigt auch das Bundeslagebild Cybercrime 2021 [18] vom Bundeskriminalamt. Laut diesem Lagebild ist die Zahl der erfassten Cyberstraftaten in den letzten Jahren immer weiter angestiegen, wohingegen die Zahl der aufgeklärten Straftaten prozentual zurückgegangen ist (siehe Abbildung 1).

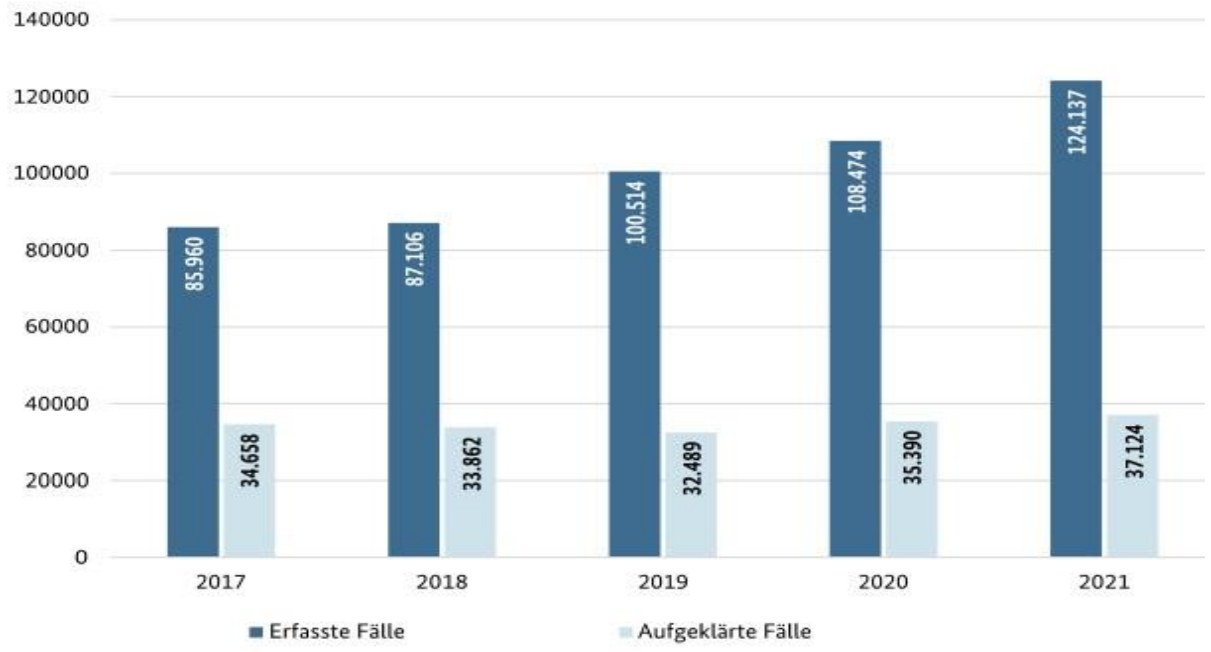

Abbildung 1: Relation zwischen erfassten und aufgeklärten Cybercrime-Fällen in Deutschland von 2017 bis 2021 [18]

Laut dem Jahresbericht des Bundesamtes in der Informationssicherheit (BSI) aus dem Jahr 2022 [19] sind Cyber-Kriminelle nicht nur an großen Unternehmen, sondern auch an kleinen und mittleren Unternehmen interessiert. Das liegt möglicherweise daran, dass die größeren Unternehmen vermehrt auf den Einsatz von IT-Sicherheitslösungen setzen und es den Cyber-Kriminellen so deutlich schwieriger machen [20], während bei KMU noch keine oder wenige

Informationssicherheitslösungen vorhanden sind und daher Cyberangriffe leichter als bei größeren Unternehmen vorgenommen werden können.

Eine repräsentative Umfrage, die vom TÜV-Verband in Auftrag gegeben und vor kurzem veröffentlich wurde, in der Unternehmen mit zehn bis zu 249 Mitarbeitenden befragt wurden, ergab, dass es 2022 zu mindestens 50.000 Informationssicherheitsvorfällen gekommen ist. Aus der Studie geht hervor, dass sich fast sechs von zehn Befragten von Cyberangriffen bedroht fühlen und etwa zwei von drei Befragten der Meinung sind, dass Unternehmen verpflichtet werden sollten, in die eigene Informationssicherheit zu investieren [21, 22].

Unternehmen mit mehr als 250 Mitarbeitenden verfügen meist über ausreichend Ressourcen (materiell und personell), um Informationssicherheitslösungen in ihren Unternehmen zu integrieren. Die grundlegenden Gedanken und Anforderungen sind hierfür in den Normen der Normenfamilie DIN EN ISO/IEC 27000 [23–25] zusammengefasst. Für KMU gelten besondere Anforderungen, weshalb diese in speziellen Normen und Richtlinien (u. a. VdS 10000 [26] und VdS 10005 [27]) erfasst wurden.

Damit KMU ein ISMS erfolgreich auf der Grundlage der o. g. Normen in Verbindung mit ihren Besonderheiten als KMU implementieren können, wurde in dieser Arbeit ein Leitfaden entwickelt. Er soll dazu dienen, dass diese Unternehmen durch den Aufbau und die Implementierung eines Informationssicherheitsmanagementsystems geleitet werden, um dadurch in ihrem jeweiligen Unternehmen ein ausreichendes Maß an Informationssicherheit gewährleisten zu können.

1.2 Beschreibung der Aufgabenstellung

Die Aufgabenstellung (angehängt in Anhang B) sieht die Entwicklung eines Leitfadens für die Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen vor.

Im Rahmen des Projektes „Mittelstand-Digital-Zentrum Hannover“ werden derzeit kostenfreie Angebote für kleine und mittlere Unternehmen erstellt, um diese Unternehmen bei der Digitalisierung der Unternehmensprozesse zu unterstützen. In diesem Projekt wird ein Workshop entwickelt, der es KMU ermöglicht, die Grundlagen eines ISMS kennenzulernen und zu verstehen. Für die langfristige Unterstützung von KMU wird mit der vorliegenden Arbeit ein Leitfaden entwickelt, welcher den Unternehmen die Umsetzung von Informationssicherheit in Form eines roten Fadens bzw. einer Checkliste erleichtern soll.

Dieser Leitfaden ist so zu gestalten, dass er branchenübergreifend angewendet werden kann.

Anhand von Normen und Standards und zugehöriger Sekundärliteratur soll der aktuelle Stand der Normen und technischen Standards erfasst und analysiert werden. Hierzu wird besonderes Augenmerk auf die Normenfamilie DIN EN ISO/IEC 27000 und insbesondere die VdS-Richtlinien gelegt. Auf dieser Basis soll im Anschluss der Leitfaden erstellt werden.

1.3 Aufbau der Arbeit

In Kapitel 2 wird zunächst der Stand der aktuellen Normen sowie der technischen Standards thematisiert. Eine ausführliche Beschreibung der für diese Arbeit relevanten Normen und Richtlinien erfolgt in den beiden darauffolgenden Kapiteln 3 und 4.

Die Grundlage dieses Leitfadens sind die Normen der DIN EN ISO/IEC 27000er Normenfamilie, die beiden Richtlinien VdS 10000 und VdS 10005 der VdS Schadensverhütung, sowie die Standards und Leitlinien des Bundesministeriums für Sicherheit in der Informationstechnik (BSI).

In Kapitel 3 werden anhand der Normen DIN EN ISO/IEC 27000 [23], DIN EN ISO/IEC 27001 [24] und DIN EN ISO/IEC 27002 [25] aus der Normenfamilie der DIN EN ISO/IEC 27000er Reihe Art und Aufbau eines ISMS erklärt.

Die VdS-Richtlinien VdS-10000 [26] und VdS-10005 [27] beschreiben die Implementierung eines Informationssicherheitsmanagementsystems in kleinen und mittleren Unternehmen mit weniger als 250 Mitarbeitenden und sind in Kapitel 4 zu finden. In Kapitel 5 wird ein Leitfaden allgemein beschrieben. Es wird näher darauf eingegangen, wie ein Leitfaden aufgebaut und genutzt werden kann. Die Konkretisierung des Leitfadens zur Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen erfolgt in Kapitel 6. Zum Abschluss dieser Arbeit erfolgt ein Schlusswort mit einem Ausblick auf mögliche Erweiterungen des Leitfadens.

1.4 Definition der KMU und Adressaten des Leitfadens

Im folgenden Dokument sind bei Erwähnung von kleinen und mittleren Unternehmen auch die sehr kleinen Unternehmen inbegriffen. Diese stellen lediglich eine Besonderheit der kleinen Unternehmen dar und sind daher im Laufe der Arbeit dem Begriff der kleinen Unternehmen immanent.

Der Leitfaden beschreibt die Einführung eines ISMS bei

- sehr kleinen Unternehmen[1],
- kleinen Unternehmen und
- mittleren Unternehmen.

Diese Einteilung folgt einer Empfehlung der europäischen Kommission von 2003 [8].

Danach beschäftigen sehr kleine Unternehmen weniger als **zehn** Mitarbeitende und haben eine maximale Jahresbilanzsumme von **zwei** Millionen Euro.

Kleine Unternehmen haben mehr Mitarbeitende als sehr kleine Unternehmen, aber weniger als **50** und die Jahresbilanzsumme übersteigt nicht die Grenze von **zehn** Millionen Euro.

[1] Häufig wird in der Literatur von Kleinstunternehmen statt sehr kleinen Unternehmen gesprochen. Aus Gründen der Übersichtlichkeit und Einheitlichkeit wird in dieser Arbeit von dieser Bezeichnung abgesehen.

Mittlere Unternehmen beschäftigen mehr als Kleinunternehmen, aber weniger als **250** Mitarbeitende und haben eine maximale Jahresbilanzsumme von **43** Millionen Euro.

Dieser Leitfaden richtet sich an Geschäftsleitungen und fachlich zuständige Personengruppen von kleinen und mittleren Unternehmen. Diese legen die langfristige Unternehmenspolitik fest, bestimmen die strategischen Ziele und setzen entsprechende Pläne und Strukturen um [16]. Bei kleineren Unternehmen ist die Geschäftsleitung vertreten durch den Geschäftsführer oder den Inhaber. In der folgenden Arbeit wird der Begriff Geschäftsleitung gleichbedeutend für die verschiedenen Bezeichnungen wie Geschäftsführer(in), Inhaber(in), Top-Management oder geschäftsführende Direktion verwendet, die in den Normen, Richtlinien und der Literatur Anwendung finden.

Der Leitfaden richtet sich an alle Unternehmen, die unter die zuvor dargestellte Definition von KMU eingruppiert werden können. Für kleine und sehr kleine Unternehmen können einige Schritte übersprungen werden. Diese Ausnahmen sind im Leitfaden besonders angemerkt. Im Leitfaden werden jedoch nicht die Besonderheiten für KRITIS-Unternehmen beleuchtet, weshalb sich dieser Leitfaden nicht an solche Unternehmen richtet, die unter die KRITIS-Einstufung fallen.

2 Aktueller Stand von Normen und technischen Standards

Die Entwicklung von Verfahren für die Informationssicherheit von Unternehmen erfordert einen detaillierten Kenntnisstand über den aktuellen Stand der Technik sowie deren Normen, Richtlinien und Standards.

Normen werden durch nationale und internationale Organisationen erstellt und verwaltet. Normen, die weltweite Gültigkeit besitzen, werden üblicherweise durch die ISO (International Standard Organization – Internationale Organisation für Normung) veröffentlicht und vertrieben. Jede interessierte Mitgliedsorganisation hat Zugang zu den einzelnen Komitees und kann an der Normenentwicklung mitwirken. Bei elektrotechnischen Themen arbeitet die ISO eng mit der IEC (International Electronical Commission – Internationale Elektrotechnische Kommission) zusammen. Im Folgenden wird auf die wesentlichen Normen und Veröffentlichungen, welche den Themenkomplex betreffen, näher eingegangen.

Dieses Kapitel gibt einen kurzen Überblick über die Normen der DIN EN ISO/IEC 27000er-Familie und die Richtlinien der „VdS Schadensverhütung GmbH“. Weiterhin wird auf die Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und andere relevante Literatur eingegangen.

2.1 Normenfamilie DIN EN ISO/IEC 27000

Die Normen der DIN EN ISO/IEC 27000er Familie beschreiben ein Informationssicherheitsmanagementsystem (ISMS) – ein Sicherheitsverfahren in der Informationstechnik.

Entstanden ist die DIN EN ISO/IEC 27000er Familie aus dem 1995 (siehe Abbildung 2) von der britischen Regierung in Zusammenarbeit mit der British Standard Institution entwickelten Standard BS 7799 [29]. Das Ziel dieses Standards war es, den Führungskräften und Mitarbeitenden eines Unternehmens ein Modell zur Verfügung zu stellen, das die Einführung und den Betrieb eines effektiven ISMS ermöglicht. Der BS7799 bestand aus zwei Teilen und bildet die Grundlage der heutigen DIN EN ISO/IEC 27000er Normenfamilie.

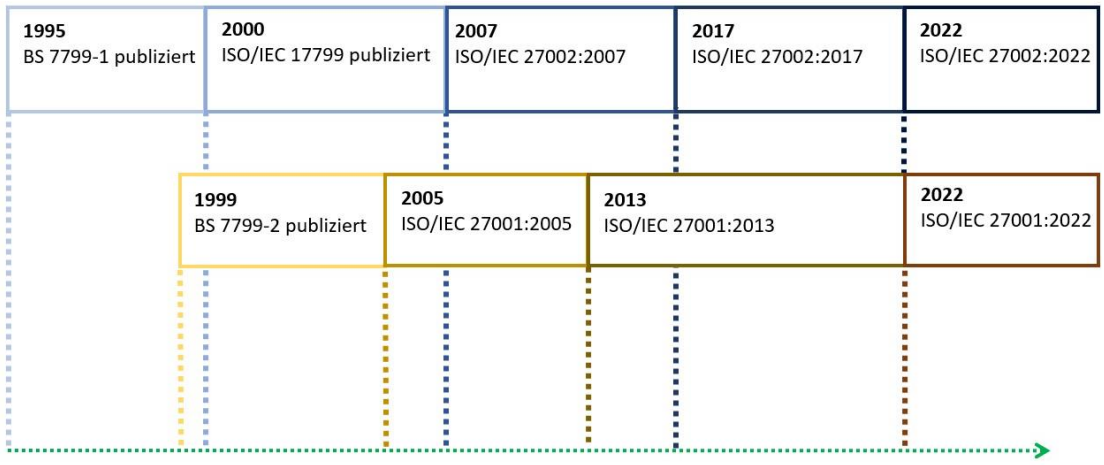

Abbildung 2: Historische Entwicklung der ISO Normen 27001 und 27002 vgl. [28]

Nach der Überarbeitung, einer Prüfung und Genehmigung durch die internationale Organisation für Normung wurde der zweite Teil des BS 7799 nahezu unverändert im Oktober 2005 als internationale Normung **ISO/IEC 27001** veröffentlicht. Drei Jahre später erfolgte die Übernahme der Norm in den deutschen DIN-Katalog und somit auch die deutsche Übersetzung (DIN ISO/IEC 27001). Auch diese Norm wurde seit der ersten Veröffentlichung weiterentwickelt, sodass die aktuellste Überarbeitung aus dem Jahr 2022 stammt (ISO/IEC 27001:2022) [30, S. 17].

2007 erfolgte die Veröffentlichung des ersten Teils des BS 7799 weitestgehend unverändert durch die ISO und die Aufnahme der Norm in die ISO/IEC 27000er Reihe. Seit der ersten Veröffentlichung ist auch diese Norm weiterentwickelt worden. Die Version aus dem Jahr 2017 wurde überarbeitet und in der novellierten Fassung im Oktober 2022 durch die Prüfungskommission als **ISO/IEC 27002**:2022 veröffentlicht.

Das Sekretariat dieser Normenfamilie wird vom DIN-Normenausschuss (Deutsches Institut für Normung) gehalten. Neben den drei eben erwähnten ISO Normen sind noch weitere speziellere Normen in der Normenfamilie ISO/IEC 27000 enthalten. Diese sind in der nachfolgenden Abbildung (Abbildung 3) dargestellt. Die ausgegrauten Normen werden in der vorliegenden Arbeit nicht berücksichtigt. Mithin werden im weiteren Verlauf die für diese Arbeit relevanten Teil-Normen der DIN EN ISO/IEC 27000er Familie kurz beschrieben.

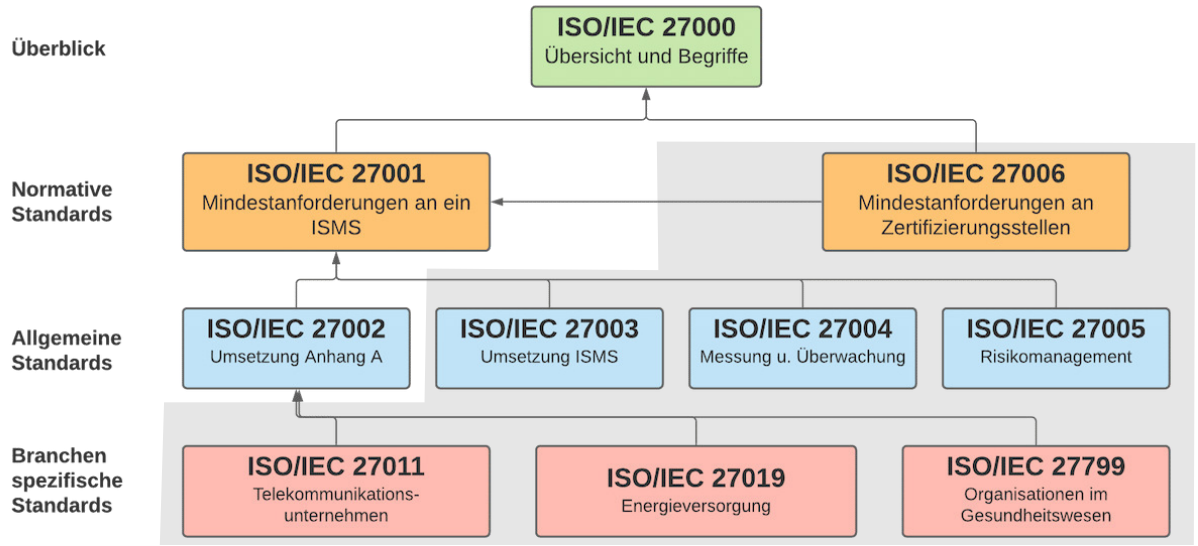

Abbildung 3: Normen der ISO 27000-Familie [31]

2.1.1 DIN EN ISO/IEC 27000

Die Norm DIN EN ISO/IEC 27000 [23] ist ein internationaler Standard und gibt einen Überblick über das Vokabular von Informationssicherheitsmanagementsystemen, die Gegenstand der Normenfamilie sind und deren Terminologie. Sie beinhaltet die dazugehörigen Begriffe und Definitionen, die üblicherweise in der ISMS-Normenfamilie verwendet werden [32].

Jedes Unternehmen kann unabhängig von der eigenen Art und Größe diese Norm anwenden.

Der aktuelle Stand dieser Norm ist die Version ISO/IEC 27000:2018. Die aktuelle deutsche Version entstand zwei Jahre später (DIN EN ISO/IEC 27000:2020).

Inhaltlich wird diese Norm in Kapitel 3.1 betrachtet.

2.1.2 DIN EN ISO/IEC 27001

In der Norm DIN EN ISO/IEC 27001 [24] sind die Anforderungen und Maßnahmen an ein ISMS in der Informationstechnik enthalten. Für Unternehmen, die eine Zertifizierung durch einen Audit anstreben, hat diese Norm unmittelbare Relevanz. Die DIN EN ISO/IEC 27001 beschreibt innerhalb der 27000er Familie den zentralen Standard [30, S. 16].

Der aktuellste Stand dieser Norm (nach zwei Korrekturversionen) ist die Version ISO/IEC 27001:2022[2]. Die aktuelle deutsche Version entstand zwei Jahre später (DIN EN ISO/IEC 27001:2017).

Eine detaillierte Betrachtung zu dieser Norm erfolgt in Kapitel 3.2.

2.1.3 DIN EN ISO/IEC 27002

Die DIN EN ISO/IEC 27002 [25] beinhaltet Informationssicherheitsmaßnahmen für die Cybersicherheit und den Schutz der Privatsphäre und ist Teil der Normenreihe 27000.

In dieser Norm sind neben der DIN EN ISO/IEC 27001 genannten Maßnahmen auch die praktischen Umsetzungen beschrieben. Neben den eben genannten Normen DIN EN ISO/IEC 27000 und DIN EN ISO/IEC 27001 ist die DIN EN ISO/IEC 27002 die wohl am häufigsten verwendete Norm in diesem Zusammenhang [30, S. 17].

Der aktuelle Stand dieser Norm ist die Version DIN EN ISO/IEC 27002:2022.

In Kapitel 3.3 wir diese Norm detaillierter betrachtet.

[2] Aktuell liegt eine Entwurfsversion aus April 2023 [33] vor. Da es sich hierbei lediglich um eine Entwurfsversion handelt, ist diese Entwurfsversion **nicht** Teil der Arbeit.

2.2 Richtlinienfamilie VdS Schadensverhütung

Die VdS Schadensverhütung (ehemaliger Verband der Sachversicherer) legt in seinen Richtlinien (Abbildung 4) Mindestanforderungen an die Informationssicherheit für kleine und mittlere Unternehmen fest und beschreibt damit ein an KMU angepasstes Informationssicherheitsmanagementsystem. Nur auf der Basis der Vorgaben dieser Dokumente ist eine Zertifizierung durch die VdS Schadensverhütung möglich.

Durch diese Zertifizierung wird bestätigt, dass die organisatorischen, technischen und präventiven Abläufe durch geeignete Reaktionen und Maßnahmenkataloge auf die wichtigsten Angriffsszenarien angepasst sind. Mit der Zertifizierung durch die VdS Schadensverhütung können sich daher Unternehmen, Lieferanten/Lieferantinnen, Kunden/Kundinnen uvm. gegenseitig Vertrauen in die Informationssicherheitstechnik bescheinigen, sodass u.a. die ausgetauschten Daten nach der durch die VdS angepassten Datenschutzverordnung (VdS 10010) geschützt werden. Die Zertifizierung erleichtert auch den Abschluss einer Versicherung gegen eintretende Schäden aufgrund von Cyberangriffen. Laut dem Bundesamt für Sicherheit in der Informationstechnik stellt u.a. die VdS 10000 (Kapitel 2.2.1 und 4) neben der DIN EN ISO/IEC 27001 (vgl. Kapitel 2.1.2 und 3.2) und dem BSI-Grundschutz eine gute Grundlage für die Implementierung eines Informationssicherheitsmanagementsystems in kleinen und mittleren Unternehmen dar [34].

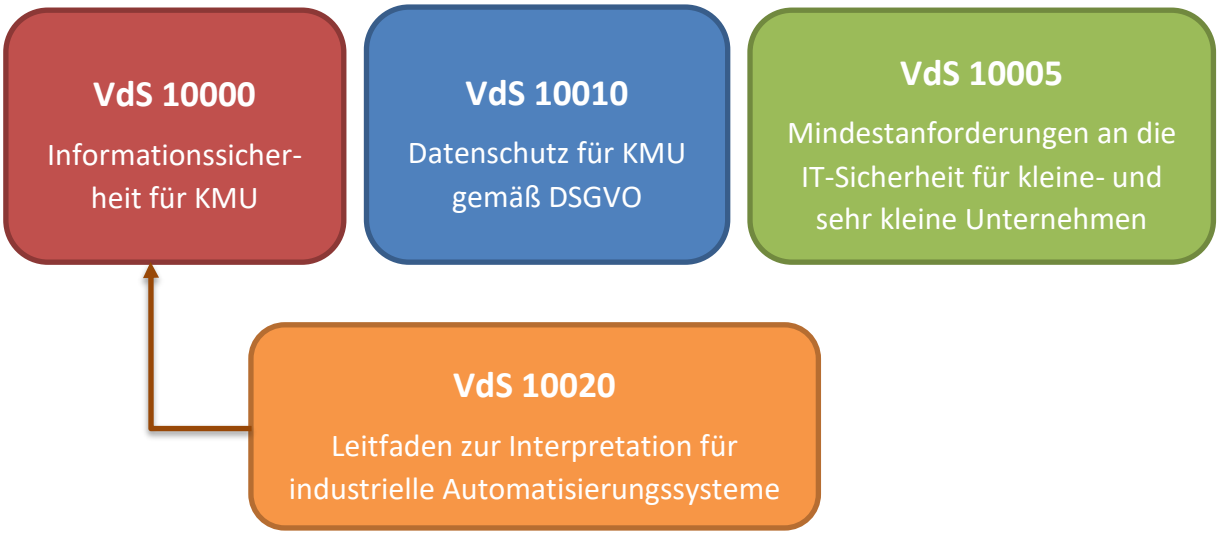

Abbildung 4: Übersicht VdS-Richtlinien

2.2.1 VdS 10000

Die Richtlinie VdS 10000 [26] ist branchenneutral formuliert und beinhaltet Maßnahmen, die speziell auf KMU angepasst sind. Dadurch kann die Informationssicherheit des jeweiligen Unternehmens mit speziell auf das Unternehmen zugeschnittenen Maßnahmen sichergestellt werden. Für KMU ist es wichtig, dass die Anforderungen an ein ISMS nicht zu einer Überforderung im organisatorischen und finanziellen Bereich führen. Die VdS Schadensverhütung gibt an, dass mithilfe der VdS 10000 der Arbeitsaufwand, ein ISMS in einem KMU zu implementieren, um 80% sinkt [34].

Durch den geregelten Prozess, der in dieser Richtlinie beschrieben wird, ist der Aufbau eines ISMS erleichtert. Neben der VdS 10000 ergänzt die VdS 10020 die Implementierung eines ISMS für industrielle Automatisierungssysteme. In ihr sind Interpretationen und Umsetzungsvorschläge als Leitfaden zusammengefasst. Die VdS 10020 ist nicht Bestandteil dieser Arbeit.

Durch eine mögliche Zertifizierung nach der VdS 10000 ergeben sich für KMU eine Reihe von Vorteilen [34].

Durch das Zertifikat

- wird bestätigt, dass das Unternehmen sich präventiv auf die wichtigsten Angriffsszenarien technisch und organisatorisch vorbereitet hat.
- wird die Unternehmenssicherheit im Bereich des Risikomanagements um den Aspekt der Informationssicherheit erweitert.
- kann das Unternehmen eine zweite Verteidigungslinie aufbauen, in dem das Restrisiko an einen darauf spezialisierten Versicherer übertragen wird. Die VdS Schadensverhütung genießt schon seit mehr als 100 Jahren das Vertrauen der Sachversicherer.
- wird die Risikotransparenz im Unternehmen erhöht. Diese Transparenz entlastet die Inhaber/Inhaberin und diese können sich dadurch wieder auf ihre Kernaufgaben konzentrieren.
- wird gegenüber den externen Stakeholdern/Stakeholderinnen gezeigt, dass die verwendeten Informationen geschützt sind und Risiken zur Einschränkung der Lieferfähigkeit vermindert wurden.

Neben all diesen direkten Vorteilen entstehen Wettbewerbsvorteile des Unternehmens gegenüber nicht zertifizierten Konkurrenten, da diese derartige Sicherheitszusicherungen im Bereich der Informationssicherheit möglicherweise nicht machen können.

Eine detaillierte Beschreibung der Inhalte dieser Norm erfolgt in Kapitel 4.

2.2.2 VdS 10005

Nach der Einführung der VdS 10000 wurden viele Unternehmen anhand dieser Richtlinie zertifiziert [20]. Dabei wurde festgestellt, dass es bei kleinen Unternehmen vieler Anpassungen bedarf, da diese nicht über die Ressourcen von mittleren Unternehmen verfügen. Daher bezieht sich die VdS 10005 [27] insbesondere auf den Umgang mit Unternehmen mit weniger als 20 Mitarbeitenden. Hierbei werden einige Abgrenzungen getroffen, die bei den sehr kleinen Unternehmen nicht von Bedeutung sind bzw. aufgrund von Ressourcenmangel nicht durchgeführt werden können.

Da die VdS 10005 aus der VdS 10000 entstanden ist, ist sie aufwärtskompatibel, sodass ein kleines Unternehmen bei einer Expansion keine komplette Umstrukturierung vornehmen muss, sondern auf dem ISMS nach VdS 10005 aufbauen und die zusätzlich erforderlichen Maßnahmen der VdS 10000 zusätzlich integrieren kann [20].

In der Norm VdS 10005 wird ein kleines Unternehmen als ein Unternehmen mit maximal 20 Mitarbeitenden beschrieben. Hiervon wird in dieser Arbeit abgewichen, da es zur Definition von sehr kleinen und kleinen Unternehmen eine Empfehlung der europäischen Union aus dem Jahr 2003 gibt [8]. Näheres zu der Aufteilung von KMU ist im Kapitel 1.4 zu finden.

Eine detaillierte Beschreibung der Inhalte der VdS 10005 erfolgt zusammen mit der VdS 10000 in Kapitel 4.

In den VdS Richtlinien sind kleine und sehr kleine Unternehmen auf 20 Mitarbeitende beschränkt. Die europäische Kommission definiert kleine Unternehmen jedoch bis hin zu 50 Mitarbeitenden. Aufgrund dieser Diskrepanz wird im Folgenden nur von **sehr kleinen**, **kleinen** und **mittleren** Unternehmen gesprochen.

2.3 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik mit Amtssitz in Bonn ist seit 1991 für die Aufklärung von und die Prävention vor Cyberangriffen zuständig und gestaltet die Informationssicherheit in der Cybersicherheitsbehörde der Bundesrepublik Deutschland. Hierbei informiert das BSI über Risiken und mögliche Schutzmaßnahmen in der Informationstechnik mit Richtlinien und Maßnahmenkatalogen wie dem IT-Grundschutz [35].

Die Grundlage der Arbeit des BSI ist das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“ (BSI-Gesetz – BSIG) [36]. Insbesondere der Schutz der Regierungsnetze und der Sicherung zentraler Netzübergänge gehören zu den Hauptaufgaben des BSI.

Das BSI hat 2009 verbindliche Grundsätze in den Sicherheitsstandards für die Beschaffung und den Einsatz von IT-Infrastruktur entwickelt. Im Jahr 2015 wurden die Aufgaben und Befugnisse des BSI durch das erste IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – IT-SiG 1.0) stark erweitert – seitdem gehört auch der Schutz der kritischen Infrastruktur (KRITIS) dazu. Zudem wurden die Betreiber von KRITIS dazu verpflichtet, jeden IT-Sicherheitsvorfall dem BSI zu melden [37].

Seit dem ersten Quartal 2021 sind die Aufgaben und insbesondere die Befugnisse des BSI durch das zweite IT-Sicherheitsgesetz (IT-SiG 2.0) [38] erneut erweitert worden. Das BSI ist nicht nur für den Schutz sämtlicher Regierungsnetze zuständig, sondern ist auch dazu ermächtigt, diesen Schutz zu kontrollieren und zu prüfen. Jedes Digitalisierungsvorhaben des Bundes oder der Länder ist mit dem BSI abzustimmen.

Mit dem zweiten IT-Sicherheitsgesetz ist auch der digitale Verbraucherschutz im BSI verankert. Hierfür berät das BSI Verbraucherinnen und Verbraucher u. a. zu den Themen Risikobewertung von Technologien, Produkten und Dienstleistungen.

Das Bundesamt für Sicherheit in der Informationstechnik gibt seit über 25 Jahren die bewährten Methoden des IT-Grundschutzes heraus. Hiermit kann ein auf das eigene Unternehmen passgenaues Informationssicherheitsmanagementsystem etabliert werden. Das BSI bezieht sich hierbei nicht nur auf KMU, sondern auf alle Unternehmensgrößen.

Der IT-Grundschutz setzt sich aus vier BSI-Standards und dem IT-Grundschutz-Kompendium zusammen. Alle dienen als Grundlage für eine wirksame Informationssicherheit.

2.3.1 BSI-Standards

In den vier BSI-Standards sind Aufgaben und Standards beschrieben, wie ein ISMS in einem Unternehmen aufgebaut bzw. etabliert werden kann.

Die ursprünglichen BSI-Standards laufen unter der Nummer 100-**X**, werden jedoch nach und nach durch modernere und überabeitete Versionen ersetzt. Diese laufen unter der Nummer 200-**X**.

Diese Standards richten sich hauptsächlich an Informationssicherheitsverantwortliche, -beauftragte, -experten und -expertinnen und -beratende. Sie stehen jedoch auch anderen Informationssicherheitsinteressierten zur Verfügung.

2.3.1.1 BSI 200-1: Managementsysteme für Informationssicherheit

Der Standard beinhaltet die allgemeinen Anforderungen an ein Informationssicherheitsmanagementsystem sowie generische Anforderungen an ein Notfallmanagement. In ihm wird beschrieben, welche Faktoren für den Erfolg eines ISMS verantwortlich sind, wie das ISMS gesteuert und überwacht werden kann, wie Sicherheitsziele und die Maßnahmen zur Erreichung dieser entwickelt werden können und wie das erreichte Sicherheitsniveau gehalten und ausgebaut werden kann.

2.3.1.2 BSI 200-2: IT-Grundschutz-Methodik

Der Standard BSI 200-2 [39] ist neben dem BSI-200-1 und BSI-200-3-Standard einer der drei elementaren Bausteine des IT-Grundschutz-Kompendiums (siehe auch 2.3.2). In ihm sind die Grundlagen der Vorgehensweise und des Aufbaus eines ISMS beschrieben. IT-Verantwortliche können mithilfe dieses Standards ein ISMS aufbauen, überprüfen und erweitern. Das Ziel dieses Standards ist die Reduzierung des Aufwandes zum Aufbau eines ISMS.

2.3.1.3 BSI 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

Der dritte elementare Baustein des IT-Grundschutzes ist die Risikoanalyse. Diese wird im BSI 200-3-Standard [5] detailliert beschrieben. Der Standard bündelt die risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.

2.3.1.4 BSI 200-4: Business Continuity Management

Der BSI 200-4 [40] ist zurzeit nur als Community-Draft verfügbar. Community-Draft bedeutet, dass der Standard vom BSI noch nicht final veröffentlicht wurde und den Anwendenden bis zu diesem Zeitpunkt die Möglichkeit gegeben wird, Feedback zu geben. Aus diesem Grund ist der Vorgänger (BSI 100-4) [41] der aktuell gültige Standard. Dieser ist seit Jahren eine fundierte Hilfestellung im Bereich des Notfallmanagements. Im Laufe der Jahre wurde deutlich, dass durch diverse Entwicklungen und Erfahrungen in diesem Bereich der Standard aktualisiert werden muss. Mit dem überarbeiteten Standard erhalten Anwendende einen leichteren Einstieg in die Thematik rund um das Business Continuity Management.

Wird der BSI 200-4 Standard final veröffentlicht, löst er den älteren 100-4 Standard ab. In dieser Arbeit wird die neuere und noch nicht final freigegebene Version verwendet.

2.3.2 (BSI) IT-Grundschutz-Kompendium

Im IT-Grundschutz-Kompendium [42] sind etwa 100 Bausteine enthalten, die Anwendenden erklären, wie ein System nach außen hin abgesichert werden sollte. Hierunter fallen nicht nur technische, sondern auch organisatorische und personelle Aspekte. Diese können durch die/den Anwendende(n) situations- und unternehmensabhängig ausgewählt werden. Das IT-Grundschutz-Kompendium richtet sich vorrangig an öffentliche Einrichtungen, aber auch an private Unternehmen, mit dem Ziel, die IT-Systeme und Prozesse sicherer zu gestalten.

Das IT-Grundschutz-Kompendium beschreibt drei verschiedene Vorgehensweisen zur Absicherung der Informationssicherheit.

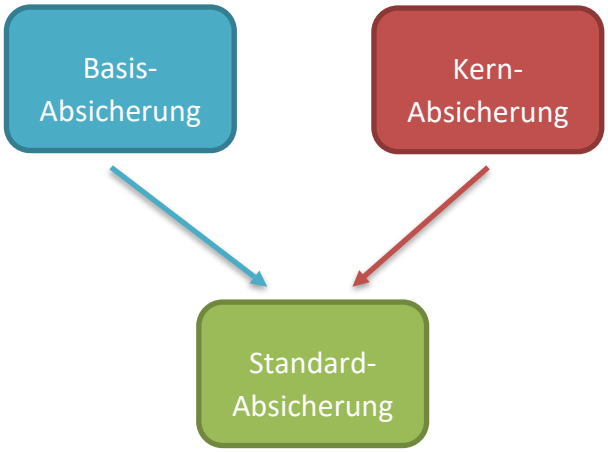

Abbildung 5: Aufbau des IT-Grundschutz-Kompendiums

- Basis-Absicherung

  Die Basis-Absicherung ist relevant für KMU, indem Mindestanforderungen (bspw. Firewalls und Zugangsbeschränkungen) definiert und umgesetzt werden.

- Kern-Absicherung

  Mit der Kern-Absicherung können Unternehmen ihre Daten (insb. Kunden- und/oder Produktionsdaten) schützen.

- Standard-Absicherung

  Die Standard-Absicherung ist die Fortsetzung der beiden vorherigen Absicherungen und hebt die Informationssicherheit auf eine neue Ebene. Hiermit kann der Informationssicherheitsbeauftragte die Assets und Prozesse des Unternehmens umfassend schützen.

2.4 DIN SPEC 27076: Standard zur IT-Sicherheitsberatung für kleine Unternehmen

Neben der DIN EN ISO/IEC 27000er-Normenfamilie, den VdS-Richtlinien VdS 10000 und VdS 10005 und den BSI-Standards, existieren noch weitere Standards im Bereich Informationssicherheit. Einer dieser Standards ist in der DIN SPEC 27076 [43] zu finden.

In diesem Standard, der im Mai 2023 veröffentlich wurde, werden Anforderungen an die Informationssicherheit für kleine und sehr kleine Unternehmen festgelegt, auf die externe Dienstleistungsunternehmen im Bedarfsfall zurückgreifen können.

Dieser Standard stellt für externe Dienstleistende einen Leitfaden zur Verfügung, der bei Beratungsgesprächen zu Hilfe genommen werden kann.

Der Leitfaden gliedert sich in vier Bereiche:

- Einholen der Erstinformationen des zu beratenden Unternehmens

  Hierbei erfolgt ein Vorgespräch zwischen dem/der IT-Dienstleister(in) und dem Unternehmen, bei welchem u. a. der grobe Ablauf des Beratungsprozesses, der Ressourceneinsatz und die groben Themenbereiche besprochen werden.

- Erhebung des IST-Zustandes

  An der Erhebung des IST-Zustandes sollte die gesamte Geschäftsleitung des Unternehmens teilnehmen. In diesem Gespräch geht es um die Erfassung des tatsächlichen IST-Zustandes des Unternehmens. Daher gibt es keine richtigen oder falschen Antworten seitens des Unternehmens in Bezug auf Informationssicherheit.

  Das Gespräch ist für den/die IT-Dienstleister(in) rein informativ. Es werden hier noch keine beratenden Aspekte artikuliert.

- Auswertung der erhobenen Daten und Erstellung eines Berichts

  Im dritten Schritt werden die vorher ermittelten Daten durch den/die IT-Dienstleister(in) ausgewertet sowie bewertet und schließlich in einem Ergebnisbericht zusammengefasst.

- Präsentation des Berichts und Bekanntgabe von Handlungsempfehlungen

  Im letzten Schritt des Beratungsprozesses, stellt der/die IT-Dienstleister(in) den Ergebnisbericht vor und gibt seine/ihre Handlungsempfehlungen gemäß des Ergebnisberichtes bekannt.

Im Anhang dieses Standards ist eine Tabelle zu finden, welche die Leitfragen und dazugehörige Handlungsempfehlungen beinhaltet. Diese kann der/die beauftragte IT-Dienstleister(in) in einem Gespräch zur Erhebung des IST-Zustandes nutzen, sofern diese für das Unternehmen relevant sind.

2.5 Zusammenfassung

In Kapitel 2 wurden die wichtigsten Normen, Richtlinien und andere Veröffentlichungen zum Thema Informationssicherheitsmanagementsystem im Allgemeinen und im Besonderen in Bezug auf KMU vorgestellt.

Für den zu erstellenden Leitfaden sind hauptsächlich die beiden Richtlinien der VdS (VdS 10000 und VdS 10005) relevant, da insbesondere diese sich auf KMU beziehen. Die Normen der Normenfamilie DIN EN ISO/IEC 27000 helfen jedoch, das Thema ISMS im nächsten Kapitel zu erklären und sind auch in Teilen für größere KMU relevant.

Neben der Normenfamilie der DIN EN ISO/IEC 27000 und den Richtlinien der VdS wurden auch die Werkzeuge des Bundesamtes für Sicherheit in der Informationssicherheit und die im Mai 2023 erschienene DIN SPEC 27076 beschrieben.

Die DIN SPEC 27076 richtet sich hauptsächlich an externe Dienstleistungsunternehmen und wurde daher nur der Vollständigkeit halber aufgeführt. Sie ist aber auch für KMU ein hilfreiches Dokument mit vielen Leitfragen und potentiellen Lösungsvorschlägen zur Sicherung der Informationssicherheit in einem Unternehmen.

Auf die Werkzeuge des BSI wird im Leitfaden an der ein und anderen Stelle verwiesen, da diese Dokumente sehr hilfreich sind, von einer Bundesbehörde stammen und kostenfrei öffentlich zugängig sind.

3 Was ist ein Informationssicherheitsmanagementsystem (ISMS)?

Im vorherigen Kapitel wurde der aktuelle Stand von Normen und technischen Standards vorgestellt. Die beschriebenen Normen der DIN EN ISO/IEC 27000-Familie werden in diesem und die der VdS Richtlinien in dem nächsten Kapitel (Kapitel 4) aufgegriffen und detaillierter in Bezug auf KMU betrachtet. Dabei geht es in diesem Kapitel um die Grundlagen und Anforderungen an ein ISMS im Allgemeinen.

Ein Informationssicherheitsmanagementsystem beruht auf Richtlinien, Maßnahmen und Werkzeugen, um Risiken der Informationssicherheit zu identifizieren und kontrollieren zu können.

In der Informationstechnik existieren für die Sicherheit von Systemen mehrere Schutzziele. Die drei wichtigsten (auch CIA-Schutzziele genannt) sind:

- Vertraulichkeit (**C**onfidentiality),
- Integrität (**I**ntegrity) und
- Verfügbarkeit (**A**vailability).

Durch die Anwendung eines ISMS sollen diese Ziele erreicht werden. Weitere Schutzziele sind u.a. der Schutz der Privatsphäre und die Authentizität (siehe auch Kapitel 3.1.2).

Ist eine unautorisierte Gewinnung von Informationen ausgeschlossen, so ist das erste Schutzziel Vertraulichkeit erfüllt. Das ist dann der Fall, wenn Informationen nur von befugtem Personal einsehbar sind. Ein gutes Beispiel hierfür ist eine Arztpraxis. Die vertraulich zu behandelnden Patientendaten sind nur für ein paar wenige befugte Personen (Arzt/Ärztin und Praxispersonal) zugänglich. Wird dieser Zugang nicht missbraucht, kann von Vertraulichkeit gesprochen werden.

Kommunizieren zwei befugte Personen (bspw. Arzt/Ärztin und Patient(in) schreiben E-Mails) miteinander, so kann die Kommunikation beispielsweise durch einen „Man-in-the-Middle“-Angriff (vgl. Abkürzungsverzeichnis) kompromittiert werden. Neben der Vertraulichkeit ist hierbei auch das Schutzziel Integrität verletzt, da die Richtigkeit der Daten nicht mehr sichergestellt werden kann.

Bei der Integrität wird zwischen einer starken und einer schwachen Integrität unterschieden. Starke Integrität beschreibt den Zustand der unmöglichen Datenmanipulation. Wenn eine Manipulation nicht verhindert werden kann, diese jedoch nicht unbemerkt bleibt, wird von einer schwachen Integrität gesprochen. Um die Integrität von Daten gewährleisten zu können, stehen Authentifizierungsmaßnahmen wie bspw. ein Message Authentication Code (MAC) zur Verfügung. Hierbei wird dem geschickten Datenpaket eine Prüfsumme angefügt, deren Berechnung nur Sender und Empfänger kennen. Der Empfänger kann die Integrität der Daten abschließend bewerten, indem dieser die Prüfsumme überprüft [44].

Wird ein System beispielsweise durch viele zeitgleiche Anfragen (ein sog. Denial-of-Service-Angriff) stark eingeschränkt, so ist die Verfügbarkeit nicht mehr gewährleistet. Insbesondere bei Navigationssystemen, Online-Shops oder der Börse ist die Verfügbarkeit sehr wichtig, da

ansonsten ein Totalausfall zu befürchten ist und dies zu hohem wirtschaftlichen Schaden führen kann.

Je nach Branche bzw. Ausrichtung des Unternehmens sind diese Schutzziele unterschiedlich gewichtet. So wird wahrscheinlich

- bei einer Arztpraxis das Schutzziel **Vertraulichkeit** für die Patientendaten,
- bei einem Online-Shop oder der Börse die **Verfügbarkeit** der Server und
- bei einem Kommunikationsanbieter die **Integrität** der Daten

Priorität haben.

Ein ISMS kann für jede Gewichtung dieser drei primären Schutzziele durch Anwendung der abgeleiteten Regeln und Maßnahmen angewendet werden, ist jedoch unternehmensspezifisch anzupassen.

Jede Tätigkeit (Schritte, Regeln und Maßnahmen) im Rahmen der Einführung bzw. des Betriebes eines ISMS sollte analog oder digital dokumentiert und durch die Geschäftsleitung freigegeben werden. Strebt ein Unternehmen eine Zertifizierung an, so sind diese Maßnahmen zwingend erforderlich. Zusätzlich erhöht die Dokumentation die Nachvollziehbarkeit der Maßnahmen für das ISMS.

3.1 Grundlagen eines ISMS

Die Grundlagen eines ISMS sind in der DIN EN ISO/IEC 27000 [23] beschrieben.

Unternehmen jeder Art und Größe

- sammeln, verarbeiten, speichern und übermitteln Daten,
- betrachten Informationen, Prozesse, Systeme, Netzwerke und Personen als wichtige Werte, die für das Erreichen der eigenen Ziele notwendig sind und
- sind mit Risiken konfrontiert, die die Funktionsfähigkeit und Wirtschaftlichkeit ein- und beschränken können.

All diese Informationen werden zum Beispiel durch Angriffe, Fehler oder Naturereignisse bedroht. Die Informationsrisiken und die Wirksamkeit von Maßnahmen gegen Angriffe verändern sich in der heutigen Zeit fortlaufend. Aus Medienberichten verstärkt sich der Eindruck, dass die Bekämpfung dieser Risiken immer wichtiger wird, da die Angreifenden zahlenmäßig den Verteidigenden überlegen sind und diese flexibel und mit einfachen Mitteln großen Schaden anrichten können. Daher ist es von Bedeutung, die Wirksamkeit von Maßnahmen gegen Angriffe zu überwachen, das Identifizieren von Risiken als fortlaufenden Prozess zu betrachten, diese Risiken neu zu analysieren und ggf. eine angemessene Maßnahme auszuwählen und diese ggf. entsprechend anzupassen.

Ein Informationssicherheitsmanagementsystem

- umfasst Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die von einem Unternehmen im Sinne der Informationssicherheit gesteuert werden.
- bildet ein systematisches Modell für die Einführung, Umsetzung, den Betrieb, die Überwachung, Überprüfung, Pflege und Verbesserung der Informationssicherheit.
- basiert auf einer gründlichen Risikobewertung und dient zum angemessenen Umgang mit eben diesen Risiken.

3.1.1 Voraussetzungen und Grundsätze

Für die erfolgreiche Umsetzung eines Informationssicherheitsmanagementsystems sind elementare Grundsätze notwendig.

Zuallererst muss in dem Unternehmen das Bewusstsein für die Notwendigkeit eines solchen Systems vorhanden sein. Ohne dieses ist die Einführung eines ISMS von vornherein zum Scheitern verurteilt, da ein Unternehmen nur dann sicher sein kann, wenn auch das schwächste Glied in der Kette (schwächste Teil im System) die notwendigen Inhalte verinnerlicht hat und diese lebt [45].

Die Leitung eines Unternehmens muss bereit sein, Verantwortung in Bezug auf die Informationssicherheit abzugeben bzw. auf andere zu übertragen. Es besteht jedoch zu jeder Zeit eine Verpflichtung zur Einbeziehung der Geschäftsleitung.

Die ehrliche Risikobeurteilung zur Bestimmung von angemessenen Maßnahmen ist elementar, um die Risiken des Unternehmens in Bezug auf Cyber-Angriffe individuell minimieren zu können.

Um ein ISMS einführen zu können, muss der Bereich Informationssicherheit als eigenständiger und grundlegender Bestandteil der Informationsnetze bzw. deren -systeme in die Unternehmensstruktur aufgenommen werden.

In diesem Bereich muss eine ganzheitliche Herangehensweise zum Erkennen und zur Prävention von Informationssicherheitsvorfällen gewährleistet sein.

Das Unternehmen sollte darüber hinaus eine stetige Neubewertung und Verbesserung der eigenen Systeme durchführen.

3.1.2 Begrifflichkeiten

Zum besseren Verständnis eines ISMS sind folgende Begriffe von entscheidender Bedeutung.

3.1.2.1 Information und Informationssicherheit

Informationen sind Werte wie andere Wirtschaftsgüter, die z. B. entscheidend sind für den wirtschaftlichen Erfolg eines Unternehmens. Es sind besonders schutzbedürftige Güter.

Zum Speichern von Informationen gibt es drei unterschiedliche Speicherformen.

- Analog:
  Eine analoge Speicherung von Daten erfolgt beispielsweise durch das Speichern von Daten auf Papier (z. B. Kassenbücher oder Karteikarten). Analoge Daten müssen physisch übergeben werden.
- Digital:
  Im Rahmen der fortschreitenden Digitalisierung werden Daten vermehrt digital gespeichert. Der Platzbedarf, die Handhabung und die Verwendung werden dadurch vereinfacht.
- Mental:
  Die dritte Speicherform ist weder analog noch digital. Das Fachwissen von Mitarbeitenden stellt auch eine Form der Datenspeicherung dar. Eine Übermittlung von Informationen erfolgt durch das direkte Gespräch zwischen Personen.

Die Informationssicherheit soll die drei primären Schutzziele **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** durch die Handhabung von angemessenen Sicherheitsmaßnahmen sicherstellen. Neben diesen drei primären Schutzzielen gibt es weitere, die im Laufe dieses Kapitels erklärt werden.

Das Ziel der Informationssicherheit ist anhaltender geschäftlicher Erfolg durch die Sicherstellung des kontinuierlichen Geschäftsbetriebes. Dies wird durch Maßnahmenkataloge des ISMS unterstützt und gesteuert.

3.1.2.2 Management

Das Management – im weiteren Verlauf des Dokumentes Geschäftsleitung genannt – ist verantwortlich für die Tätigkeiten Führung, Kontrolle und fortlaufende Verbesserung der Abläufe und handhabt, führt, überwacht und kontrolliert Ressourcen des Unternehmens. Im Verantwortungsbereich des Managements liegt auch die Zuständigkeit für die Findung und Überwachung von Entscheidungen im Bereich eines ISMS. In der vorliegenden Arbeit wird der Begriff Geschäftsleitung gleichbedeutend für die verschiedenen Bezeichnungen wie Geschäftsführer(in), Inhaber(in), (Top-)Management oder geschäftsführende Direktion verwendet (vgl. Kapitel 1.4).

3.1.2.3 Schutzziele:

Neben den drei primären Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität gibt es noch weitere, die zusätzlich zu den primären Schutzzielen nachfolgend kurz beschrieben werden.

- Vertraulichkeit
  Informationseigenschaft, die nur für einen vorher bestimmten Personenkreis frei zugänglich ist [26]

- Integrität
  Korrektheit bzw. Unversehrtheit von Informationen bzw. die korrekte Funktionsweise der Datenverarbeitung [26]

- Verfügbarkeit
  Ressourcen können wie gewohnt genutzt werden (stehen uneingeschränkt zur Verfügung) [26]

- Authentizität
  Echtheit, Überprüfbarkeit, Vertrauenswürdigkeit
  Informationen können eindeutig einer Quelle zugeordnet werden [26]

- Verantwortlichkeit
  Fähigkeit, eigenes Handeln und mögliche Folgen einzuschätzen

- Verbindlichkeit
  Eine Handlung kann einer Person eindeutig zugeordnet werden oder ist vertraglich bindend.

- Verlässlichkeit
  Etwas geschieht genauso, wie es erwartet wird.

- Prozesse
  Systeme von Tätigkeiten, die mittels der Verarbeitung von Eingaben Ergebnisse ausgeben [26]

3.1.2.4 Managementsystem

Ein Managementsystem beschreibt eine Strategie, mit der die Unternehmensziele erreicht werden können. Es umfasst:

- Organisationsstrukturen, Richtlinien, Planungstätigkeiten, Verantwortlichkeiten, Methoden, Verfahren, Prozesse und Ressourcen.

Dies ermöglicht es dem Managementsystem, dem Vertrauen der in- und externen Stakeholder/Stakeholderinnen (vgl. V) gerecht zu werden.

Zu den weiteren Zielen eines Managementsystems gehören die Verbesserung von Planungen und Tätigkeiten, die Erfüllung von Informationssicherheitszielen, die Einhaltung von Vorschriften, Gesetzen und Branchenstandards und die Förderung der fortlaufenden Verbesserung, Anpassung und Steuerung der Informationswerte.

3.1.3 Warum ist ein ISMS so wichtig?

Für die Implementierung eines ISMS und das Erreichen von Informationssicherheit ist ein Risikomanagement von entscheidender Bedeutung. Ein ISMS erfasst diese Risiken in Bezug auf materielle, menschliche und technische Bedrohungen.

Nur mithilfe einer nahtlosen Integration, einer auf das Unternehmen zugeschnittene Skalierung und einer ständigen Aktualisierung der entwickelten Prozesse ist der Betrieb eines ISMS möglich. Diese langfristige und strategische Entscheidung muss die Leitung eines Unternehmens vorgeben und mittragen.

Die Planung und Umsetzung sind abhängig von den Anforderungen und Zielen, dem Sicherheitsbedarf, den angewandten Geschäftsprozessen und der Größe des Unternehmens.

In der heutigen vernetzten Zeit werden immer häufiger private-, öffentliche und Firmennetze miteinander verbunden. Daraus entstehen Unsicherheiten und Gefahrenpotentiale in Bezug auf die Sicherheit der Informationen eines jeden einzelnen Unternehmens.

Ein Beispiel hierfür sind mobile Speicherlösungen wie USB-Sticks, die die Mitarbeitenden im in- sowie externen Bereich des Unternehmens nutzen. Beispielsweise nehmen Außendienstmitarbeitende das Produktportfolio oder eine Präsentation auf einem USB-Stick mit zu einem/einer Kunden/Kundin und stecken den USB-Stick in einen Computer des fremden Unternehmensnetzwerkes. Dieser USB-Stick darf ab diesem Zeitpunkt – ohne Virenüberprüfung – nicht mehr mit dem eigenen Unternehmensnetzwerk verbunden werden, da die Gefahr der Übertragung eines Virus zu hoch ist.

Es ist ein großes Bedürfnis, die Kontrolle über die Daten bei der Verwendung von USB-Sticks zu behalten, wobei diese Anforderung immer komplexer wird und es daher eines Managements bedarf, um diese Kontrolle auszuüben bzw. im Bedarfsfall wiederherzustellen.

Dafür sollte die Einführung eines ISMS bereits bei der Unternehmensplanung berücksichtigt werden, da eine nachträgliche Integration zumeist schwieriger und vor allem teurer sein kann.

Da wahrscheinlich die meisten existierenden kleinen und mittleren Unternehmen bislang kein ISMS in ihren Unternehmensablauf integriert haben (Zahl der Cyberangriffe steigt – [18]), ist es umso wichtiger, dass diese zur Wahrung ihrer Informationssicherheitsinteressen nachträglich ein ISMS implementieren. Die Vorteile eines ISMS liegen u.a. in standardisierten Prozessen, die vertrauliche Informationen bestmöglich gegen Bedrohungen schützen. Ein ISMS stellt ein strukturiertes Rahmenwerk zur Erfassung und Einschätzung von Informationssicherheitsrisiken, zur Auswahl und Anwendung geeigneter Maßnahmen und zur Messung und Verbesserung der Wirksamkeit dieser Maßnahmen dar.

Durch dieses strukturierte Rahmenwerk eines ISMS ist ein effektives Befolgen von gesetzlichen und behördlichen Bestimmungen einfacher. Für ein effektives ISMS ist es erforderlich, dass Prozesse fortlaufend analysiert, verbessert und neu bewertet und ggf. angepasst werden.

3.1.4 Einführung, Überwachung, Pflege und Verbesserung

Die Norm DIN EN ISO/IEC 27000 [23] gibt vor, dass die nachfolgenden Schritte regelmäßig wiederholt werden müssen:

3.1.4.1 Identifikation von Informationswerten und den damit verbundenen Informationssicherheitsanforderungen

Zuerst müssen die Anforderungen an ein ISMS bestimmt werden. Hierzu sind folgende Aspekte zu beachten:

- Welche Informationswerte sind im Unternehmen vorhanden und welchen Nutzen haben diese?
- Welche Geschäftsanforderungen an die Verarbeitung, Speicherung und Kommunikation von Daten liegen vor?
- Müssen gesetzliche, vertragliche und/oder behördliche Anforderungen berücksichtigt werden?

3.1.4.2 Bestimmung von Informationssicherheitsrisiken und deren Behandlung

Für die Beurteilung sollten die Risiken identifiziert, bewertet und priorisiert werden. Dabei muss festgelegt werden, welche Risiken akzeptiert werden können – die sogenannte Risikoakzeptanz. Diese sollte systematisch die Risikohöhen analysieren, um den Prozess zum Vergleichen der analysierten Risiken zu bestimmen.

Eine Risikobewertung sollte regelmäßig und bei jeder Veränderung des Systems durchgeführt werden, um Schwachstellen schneller finden zu können (z.B. dem Einbau neuer Hardware oder der Einstellung neuen Personals).

Eine Anleitung für die Einführung und Umsetzung eines solchen Informationsrisikomanagement ist in der DIN EN ISO/IEC 27005 nachzulesen.

Vor der Behandlung der identifizierten Risiken sollte das Unternehmen die Risikoakzeptanz bestimmen. Für jedes Risiko, welches zuvor durch die Risikoidentifikation bestimmt wurde, muss eine Risikobewertung mit ausführlicher Dokumentation durchgeführt werden.

Hierbei gibt es vier verschiedene Möglichkeiten des Umgang mit den Risiken:

1. Anwenden geeigneter Maßnahmen, um die Risiken zu minimieren
2. Bewusstes und sachliches Akzeptieren (eine vorher bestimmte Risikoakzeptanz ist hierbei vonnöten)
3. Risiken vermeiden, indem Ursachen ermittelt werden (die Möglichkeit der Nutzung von USB-Sticks wird untersagt und technisch verwehrt, indem die USB-Ports in den Computern gesperrt oder mechanisch blockiert werden)
4. Gemeinsames Teilen der Risiken mit anderen Parteien (Lieferanten/Lieferantinnen, Kunden/Kundinnen, Stakeholder/Stakeholderinnen, Versicherungen, usw.)

3.1.4.3 Auswahl und Umsetzung geeigneter Maßnahmen, um inakzeptable Risiken zu behandeln

Nach der Identifizierung, der Bestimmung und Bewertung der Risikofaktoren und der Entscheidung bezüglich der Behandlung erfolgen Maßnahmen zur Risikoreduzierung. Diese sollten das Risiko auf ein akzeptables Niveau senken und dabei folgendes beachten:

- Anforderungen und Beschränkungen durch (inter-)nationale Gesetze und Vorschriften (Beispiele: DIN EN ISO/IEC 27000 als international geltende Norm und das IT-SiG-2.0 als nationales Gesetz)
- Unternehmensziele
- Anforderungen und Beschränkungen des Betriebs
- Wahrung der Verhältnismäßigkeit zwischen den Kosten zur Umsetzung von Maßnahmen und den Kosten der Reduzierung bzw. den Kosten der Schadenbehebung
- Wahrung der Verhältnismäßigkeit zwischen der Notwendigkeit und der Eintrittswahrscheinlichkeit

Die Entwicklung von Maßnahmen zur Risikoreduzierung sollten schon beim Entwurf und der Planung eines ISMS berücksichtigt werden. Auch wenn ein ISMS sehr viele Vorteile mit sich bringt, kann keine Risikoreduzierungsmaßnahme einen hundertprozentigen Schutz garantieren. Das im Mittelpunkt stehende Ziel ist daher stets die Reduzierung von Risiken.

Zu jedem Zeitpunkt sollte eine ausführliche Dokumentation der Schritte erfolgen.

3.1.4.4 Überwachung, Wartung und Verbesserung der Wirksamkeit der Sicherheitsmaßnahmen

Für den Erfolg eines ISMS ist es wichtig, dass ein Berichtswesen eingerichtet wird, das die verantwortlichen Personen eines Unternehmens regelmäßig über alle Tätigkeiten und Sicherheitsvorfälle informiert.

Jede Verbesserung oder Veränderung des Systems muss durch die Leitung genehmigt werden.

Diese Maßnahmen zur Verbesserung schließen die folgenden Punkte ein:

- analysieren und bewerten der Situation, um das Verbesserungspotential zu erkennen
- festlegen der Ziele der Verbesserung/Veränderung
- suchen, bewerten und umsetzen von möglichen Zielen
- messen, verifizieren, analysieren und bewerten der Umsetzungsergebnisse
- formalisieren der Änderungen

3.1.5 Kritische Erfolgsfaktoren für das ISMS

Für ein erfolgreiches Implementieren eines ISMS sind die folgenden beispielhaften Faktoren ausschlaggebend.

- Informationssicherheitspolitik/-ziele/-tätigkeiten
- Ansatz und Rahmenwerte für Planung, Umsetzung, Überwachung, Aufrechterhaltung und Verbesserung der Informationssicherheit
- Erkennbare Unterstützung und Verpflichtung seitens aller Leitungsebenen
- Einvernehmen über die Anforderungen an den Schutz von Informationswerten (Risikomanagement)
- Wirksames Schulungs- und Fortbildungsprogramm zur Informationssicherheit
- Schärfen des Problem- und Gefahrenbewusstseins
- Wirksamer Prozess zur Handhabung von Informationssicherheitsvorfällen
- Wirksamer Ansatz zu Business-Continuity-Management
- Messsystem zur Bestimmung der Leistungsfähigkeit des ISMS

Ein ISMS ermöglicht es, die kritischen Erfolgsfaktoren zu erreichen.

3.2 Anforderungen aus der DIN EN ISO/IEC 27001 an ein ISMS

Wie in Kapitel 2.1.2 schon erwähnt, befasst sich die DIN EN ISO/IEC 27001 [24] mit den Anforderungen an ein Informationssicherheitsmanagementsystem. Diese Anforderungen beinhalten die Festlegung der Einrichtung, Umsetzung, Instandhaltung und durchgehenden Verbesserung eines Informationssicherheitsmanagementsystems.

Zusätzlich sind in dieser Norm Anforderungen für die Beurteilung und Behandlung von Risiken der Informationssicherheit entsprechend des individuellen Risikomanagements enthalten.

Grundsätzlich müssen für ein ISMS Dokumente erstellt, technische Maßnahmen umgesetzt, Prozesse und deren Verantwortliche definiert und betriebliche Änderungen den Mitarbeitenden des Unternehmens dargelegt werden.

Es wird als wichtig angesehen, dass das ISMS „gelebt“ und möglichst bereits bei der Unternehmensplanung miteinbezogen wird. [vgl. Vorwort46]

Um den Anwendungsbereich des Informationssicherheitsmanagementsystems zu definieren, ist ein Unternehmen verpflichtet, die Grenzen des Informationssicherheitsmanagementsystems unter Berücksichtigung der unternehmensrelevanten, internen sowie externen Inhalte, der Anforderungen der interessierten und relevanten Parteien und der Schnittstellen und Abhängigkeiten zwischen sich selbst und anderen Unternehmen festzulegen und zu dokumentieren.

3.2.1 Deming-Kreislauf (PDCA-Zyklus)

Das ISMS durchläuft bei jeder Anpassung die Form eines sich immer wiederholenden Kreislaufes. So ein Zyklus wird PDCA-Zyklus oder Deming-Kreis nach William Edwards Deming [47] genannt und beschreibt vier Phasen:

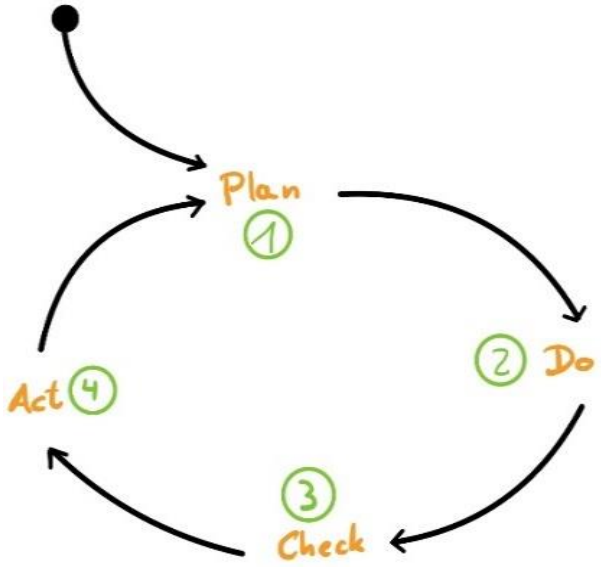

Abbildung 6: Plan-Do-Check-Act-Zyklus nach De-

Während der Planungsphase („Plan“, 1) wird der IST-Stand des Systems analysiert, das Vorgehen geplant und die Ziele werden formuliert. Dieser erarbeitete Plan enthält viele kleine Schritte, die die Vorgehensweise des Projektes darstellen. Hierfür werden die Kernprobleme erarbeitet und eine Ressourcenanalyse durchgeführt.

Ist der Plan fertiggestellt, wird er in der Durchführungsphase („Do“, 2) umgesetzt. Jeder Schritt wird gemäß der formulierten Ziele umgesetzt. Unvorhergesehene Probleme werden bestmöglich gelöst und im Zweifel offen gelassen.

In der Überprüfungsphase („Check“, 3) wird ein IST-/SOLL-Vergleich durchgeführt, ob die formulierten Ziele der ersten Phase in der zweiten Phase erfüllt wurden. Diese Phase ist mit die wichtigste der vier Phasen, da etwaige Probleme identifiziert und für den nächsten Zyklus analysiert werden können. Zudem werden in dieser Phase die Ursachen dieser Probleme ausfindig gemacht.

Die letzte Phase („Act“, 4) des sich kontinuierlich wiederholenden Deming-Kreises beschreibt die Verbesserungsphase. In den ersten drei Phasen des PDCA-Kreislaufes wurde ein Plan entwickelt, umgesetzt und überprüft. In der vierten Phase werden Verbesserungen gesucht und für die erste Phase des neuen PDCA-Zyklusses erarbeitet.

3.2.2 Führung

Die Leitungsebene in einem Unternehmen hat gemäß der DIN EN ISO/IEC 27001 verschiedene Aufgaben in Bezug auf die Einführung und den Betrieb eines Informationssicherheitsmanagementsystems.

3.2.2.1 Zeigen von Führung und Verpflichtung

Die Geschäftsleitung eines Unternehmens ist dafür zuständig, dass die Politik und die Ziele des ISMS mit der des eigenen Unternehmens vereinbar sind, diese in die Geschäftsprozesse integriert und so die Unternehmensziele erreicht werden können.

Weiterhin ist die Geschäftsleitung für die Bereitstellung der für ein ISMS benötigten Ressourcen zuständig.

Neben diesen Verpflichtungen ist die Führung auch daran interessiert, Personen in neuen Bereichen anzuleiten, bei Fragen zu unterstützen und jegliche Verbesserungen fortlaufend zu fördern, damit diese zur Wirksamkeit des ISMS beitragen können.

3.2.2.2 Festlegen einer Informationssicherheitspolitik

Die Norm DIN EN ISO/IEC 27001 legt fest, dass für die Zielrichtung der Unternehmen die Geschäftsleitung eine Informationssicherheitspolitik festlegen muss. Diese muss die Ziele und den Rahmen zur Festlegung der Informationssicherheitsziele beinhalten. In dieser Politik sind die Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit und zur fortlaufenden Verbesserung des Managementsystems enthalten. Weiterhin ist die Geschäftsleitung des Unternehmens dafür zuständig, dass die Informationssicherheitspo-

litik als dokumentierte Information jeder Person innerhalb der Unternehmen und allen interessierten Parteien (Vorstand, Lieferanten/Lieferantinnen, Kunden/Kundinnen, …) zur Verfügung gestellt wird.

3.2.2.3 Sicherstellen, dass Verantwortliche die benötigten Befugnisse bekommen

Rollen, Verantwortlichkeiten und Befugnisse im Unternehmen weist die Geschäftsleitung zu, sodass sichergestellt wird, dass das Informationssicherheitsmanagementsystem die Anforderungen der DIN EN ISO/IEC 27001 erfüllt und dass Berichte an die Leitungsebene erfolgen.

Die Ernennung einer Person oder eines/einer Dienstleisters/Dienstleisterin zum/zur Informationssicherheitsbeauftragten (ISB) muss schriftlich erfolgen.

Die Geschäftsleitung trägt dafür Sorge, dass die Person genügend zeitliche Ressourcen zur Wahrnehmung der Tätigkeiten erhält.

Zu den Tätigkeiten eines/einer ISB gehört u.a. die Koordination der Aufgaben für den reibungslosen Betrieb eines ISMS in einem Unternehmen. Weiterhin ist der/die ISB auch für die Schulung und die Fortbildungsmaßnahmen im Bereich der Informationssicherheit der Mitarbeitenden verantwortlich.

Der/Die ISB hat das Recht, an allen Projekten mit informationssicherheitsrelevanten Inhalten teilzunehmen und ggf. die Informationssicherheitsmaßnahmen des Unternehmen einzufordern.

3.2.3 Risikomanagement

Aufgabe des/der ISB ist es, relevante Bedrohungen zu identifizieren, damit diese durch geeignete Maßnahmen minimiert werden können.

Das BSI empfiehlt, am Anfang der Risikoanalyse die Prozesse im Unternehmen zu bestimmen, die für den reibungslosen Ablauf erforderlich sind. Hierfür stellt das BSI den Standard 200-2 zur Verfügung. Hierin wird die Vorgehensweise mithilfe einer Strukturanalyse erläutert [39].

Die DIN EN ISO/IEC 27001 schreibt für die Implementierung eines ISMS die Durchführung einer Risikoanalyse vor, wenn ein Unternehmen sich nach DIN EN ISO/IEC 27001 zertifizieren lassen möchte.

3.3 Informationssicherheitsmaßnahmen

Der Standard DIN EN ISO/IEC 27002 [25] ist rein informativ aufgebaut [48, S. 89]. In ihm werden verschiedene Informationssicherheitsmaßnahmen in Kategorien aufgelistet und näher erläutert. Eine detaillierte Beschreibung der einzelnen Maßnahmen ist entweder in der Norm selbst oder im Anhang A des Buches von J. Naumann [48] zu finden. Sie sind für den Leitfaden nicht relevant, können aber bei seiner Umsetzung hilfreich sein.

Die Informationssicherheitsmaßnahmen sind wie folgt kategorisiert [48, S. 5-13]:

- Organisatorische Sicherheitsmaßnahmen
    - Interne Organisation
    - Werte- und Rechteverwaltung
    - Beziehungen zu Lieferunternehmen
    - Vorfälle in der Informationssicherheit
    - Compliance
    - Interne Regeln und Dokumentation
- Personenbezogene Sicherheitsmaßnahmen
    - Vor, während und nach der Beschäftigung
    - Mobiles Arbeiten
    - Meldeprozesse
- Physische Sicherheitsmaßnahmen
    - Physische Sicherheit
    - Bedrohungen
    - Arbeitsplätze / Betriebsmittel
    - Umgang mit Werten
    - Wartung und Entsorgung
- Technologische Sicherheitsmaßnahmen
    - Zugangs-, Betriebs-, Daten-, Netz- und Entwicklungssicherheit
    - Administration
    - Netzplanaufbau
    - Änderungsmanagement
    - Technische Überprüfungen

3.4 Zusammenfassung

Im vorliegenden Kapitel wurden anhand der DIN EN ISO/IEC 27000 [23], 27001 [24] und 27002 [25] die Grundlagen eines Informationssicherheitsmanagementsystems dargestellt. Diese drei Normen beschreiben ein ISMS für jedes Unternehmen, unabhängig von der Größe. Sie beinhalten grundlegende Informationen zum Aufbau und zu den Anforderungen eines ISMS und stellen mögliche Maßnahmen für die Informationssicherheit zur Verfügung.

Mit einem Informationssicherheitsmanagementsystem lassen sich mithilfe von Normen, Richtlinien, Maßnahmen und Werkzeugen Risiken der Informationssicherheit identifizieren und kontrollieren.

Ein wirksames ISMS wird laufend wiederholt. Mithilfe des Deming-Kreislaufes kann diese Wiederholung dargestellt werden. Hierbei durchläuft das Managementsystem immer die gleichen Phasen (Plan, Do, Check, Act) und verbessert sich stetig selbst.

4 Informationssicherheitsmanagementsystem in kleinen und mittleren Unternehmen

Im vorherigen Kapitel wurden die Grundzüge und Anforderungen an ein ISMS anhand der Normen ISO/IEC 27000 [23], 27001 [24] und 27002 [25] beschrieben.

In diesem Kapitel werden die Bausteine eines ISMS mithilfe der Richtlinien VdS 10000 [26] und VdS 10005 [27] für (sehr) kleine und mittlere Unternehmen (KMU) beschrieben.

Die VdS 10000 (für kleine und sehr kleine Unternehmen: VdS 10005) ist die Grundlage für eine Zertifizierung durch die VdS Schadensverhütung. In ihr sind die Mindestanforderungen an die Informationssicherheit für kleine und mittlere Unternehmen hinterlegt. Diese Richtlinien beschreiben die erfolgreiche Implementierung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen, dem sogenannten Mittelstand, bei Verwaltungen und Verbänden.

Die VdS 10000 ersetzt die VdS 3473 und gilt seit Dezember 2018.

Die VdS 10005 entstand etwa zweieinhalb Jahre später und gilt seit Juli 2021.

4.1 Aufbau der Informationssicherheit

Der Aufbau eines Informationssicherheitsteams gemäß der Richtlinie VdS 10000 ist in dem Organigramm in Abbildung 7 dargestellt. Jede Position in diesem Organigramm muss eindeutig und widerspruchsfrei einem/einer Mitarbeitenden zugeordnet werden. Ist dies aufgrund von fehlenden personellen oder materiellen Ressourcen nicht möglich, kann in Ausnahmefällen eine Doppelbeauftragung erfolgen.

Die Richtlinie VdS 10000 fordert, dass für diese Ausnahmefälle geprüft werden muss, ob die Doppelbeauftragung rechtlich zulässig ist und ob andere Maßnahmen zur Überwachung, Kontrolle und Aufsicht ergriffen werden müssen.

In jedem Fall ist jede Besetzung einer Position zu dokumentieren und zu begründen. In dieser Dokumentation ist festzuhalten, welche Ziele jeweils erreicht werden sollen und welche Ressourcen zur Ausübung der Tätigkeiten zur Erreichung der Ziele zur Verfügung gestellt werden.

Weiterhin wird dokumentiert

- für welche Ressourcen eine Verantwortlichkeit besteht,
- welche Aufgaben zur Erreichung der Ziele erfüllt werden müssen und
- wie, wann und durch wen die Arbeit dieser Position überprüft und kontrolliert wird.

Die Zuständigkeiten und Positionen sind jährlich von dem/der Informationssicherheitsbeauftragten (ISB) zu überprüfen und zu genehmigen.

Zur Wahrnehmung der Tätigkeiten sind den jeweils zugeordneten Mitarbeitenden zeitliche Ressourcen zur Verfügung zu stellen bzw. sind sie von anderen Tätigkeiten freizustellen. Kann

eine verantwortliche Person die Aufgaben und Pflichten nicht umfänglich erfüllen, ist eine Delegation von Verantwortlichkeiten möglich. Die Gesamtverantwortung bleibt jedoch bei dem/der ursprünglich Beauftragten.

In einem Unternehmen besteht die Organisation der Informationssicherheit aus drei großen Säulen (blaue Ringstücke):

- Datenschutz und -sicherheit (meist vertreten durch Datenschutzbeauftragte)
- Belegschaft
- Geschäftsleitung.

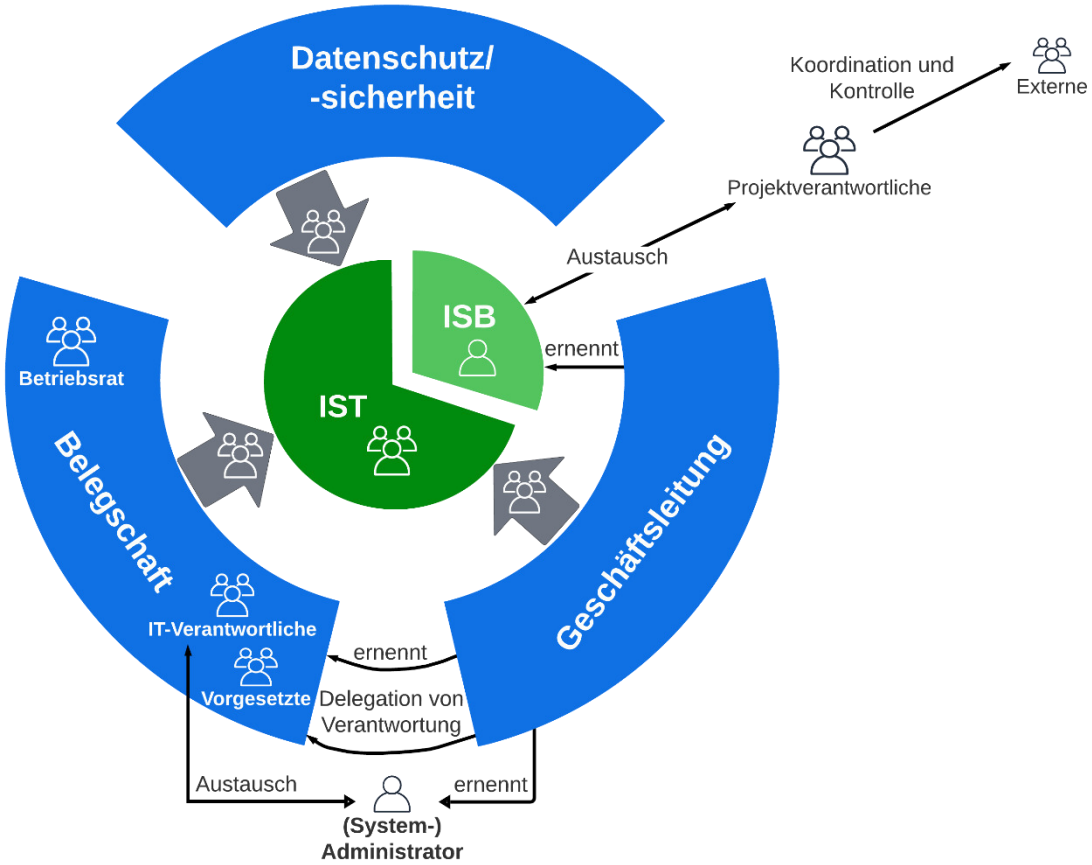

Abbildung 7: Organigramm eines Informationssicherheitsteams [49]

Alle Beteiligten entsenden vertretende Personen (dunkelgraue Pfeile) in das Informationssicherheitsteam (IST, dunkel-grüner Kreis).

4.1.1 Geschäftsleitung

Die Geschäftsleitung stellt die oberste Leitungsebene bzw. die geschäftsführende Direktion eines Unternehmens dar. Bei kleinen und mittleren, aber besonders bei sehr kleinen Unternehmen übernimmt diese Position meist der Inhaber/die Inhaberin.

Bei ihr liegt auch die Gesamtverantwortung im Bereich der Informationssicherheit. Sie ist für die Inkraftsetzung von u. a. den Informationssicherheitsrichtlinien verantwortlich. Zudem bettet sie die Informationssicherheit in die unterschiedlichen Strukturen, Hierarchien und Arbeitsabläufe des Unternehmens ein.

Zu den Aufgaben der Geschäftsleitung gehört auch die Benennung eines/einer Informationssicherheitsbeauftragten (ISB), mindestens einer Person zur (System-)Administration, mindestens eines/einer IT-Verantwortlichen (ITV) und die Bildung eines Informationssicherheitsteams (IST), dessen Aufgaben in Kapitel 4.1.4 erläutert werden.

In sehr kleinen Unternehmen muss die Geschäftsleitung nur eine mitarbeitende Person für die Umsetzung aller Richtlinien als ISB benennen [27, S. 8].

4.1.2 Belegschaft

In der Belegschaft eines KMU sind alle Mitarbeitenden eines Unternehmens zusammengefasst, die nicht zur Geschäftsleitung gehören.

Hierzu zählen insbesondere die ITV-Personen, die Vorgesetzten und die Mitarbeitenden, die ggf. durch den Betriebsrat vertreten werden.

- Die Verantwortlichen der IT-Abteilung entsenden mindestens eine Vertretung in das Informationssicherheitsteam (siehe auch Abbildung 7) und sind für die technische und organisatorische Umsetzung der Informationssicherheitsrichtlinien durch entsprechende Maßnahmen zuständig. Zusätzlich stimmen sie mit dem/der ISB alle Maßnahmen ab, die aus ihrer Sicht der Verbesserung der Informationssicherheit dienen.
- Vorgesetzte, die durch die Geschäftsleitung bestimmt werden (siehe auch Abbildung 7), um deren Aufgaben zur Schulung der Mitarbeitenden zu delegieren, müssen sicherstellen, dass die ihnen nachgeordneten Mitarbeitenden die vom Informationssicherheitsteam getroffenen technischen und organisatorischen Maßnahmen kennen und umsetzen.
- Die Mitarbeitenden sind verpflichtet, die technischen und organisatorischen Maßnahmen, die ihre Tätigkeit betreffen, einzuhalten und Störungen, Ausfälle und Sicherheitsvorfälle zu melden. Die Belegschaft entsendet mindestens eine Vertretung (ggf. ein Mitglied des Betriebsrates) in das Informationssicherheitsteam.

Die Systemadministration kann von der Belegschaft oder einem externen Dienstleistungsunternehmen wahrgenommen werden. Daher ist sie in der Grafik (Abbildung 7: Organigramm eines Informationssicherheitsteam) nicht als ständiges Mitglied der Belegschaft dargestellt.

Diese Person wird von der Geschäftsleitung bestimmt und tauscht sich mit den IT-Verantwortlichen über die zu implementierenden technischen Maßnahmen aus und sorgt im Anschluss für deren Implementierung.

4.1.3 Datenschutz / -sicherheit

Die dritte Säule der Informationssicherheit (vgl. Abbildung 7: Organigramm eines Informationssicherheitsteam) stellt der Datenschutz / die Datensicherheit dar. Dieser Bereich wird im Informationssicherheitsteam meist durch die/den Datenschutzbeauftragte(n) des Unternehmens vertreten.

Hierzu ein kurzer Auszug aus der Datenschutzgrundverordnung [50], um die Relevanz für KMU zu zeigen:

Art. 37 Absatz 1 Buchstabe b und c der Datenschutzgrundverordnung [50, Art.37 Abs. 1 b + c] legt folgendes fest:

> *„Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn…*
>
> *b) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **Durchführung von Verarbeitungsvorgängen** besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder*
>
> *c) die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen Verarbeitung** besonderer Kategorien von Daten gemäß Artikel 9 oder **von personenbezogenen Daten** über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.“*

Hieraus ergibt sich, dass die Verantwortlichen eines jeden Unternehmens (Geschäftsleitung) eine/einen Mitarbeitende(n) zum Datenschutzbeauftragten ernennen bzw. ausbilden lassen, wenn die Kerntätigkeit des Unternehmens die Verarbeitung von sensiblen Personendaten (DS-GVO Artikel 9 und 10) erforderlich macht.

Weiterhin ist ein Datenschutzbeauftragter grundsätzlich verpflichtend zu ernennen, wenn in einem Unternehmen 20 und mehr Mitarbeitende ständig mit der automatisierten Verarbeitung sensibler personenbezogener Daten beschäftigt sind [51].

Für kleine und mittlere Unternehmen sieht die Datenschutzgrundverordnung prinzipiell keine Ausnahmen vor (Europäische Datenschutzvorschrift [50]). Jedoch sind einige Pflichten und Maßnahmen nicht auf KMU und insbesondere sehr kleine Unternehmen anwendbar und können daher entfallen (Bspw. sind Mitarbeitende von KMU in den meisten Fällen nicht verpflichtet ein Verzeichnis ihrer Verarbeitungstätigkeiten in Bezug auf personenbezogene Daten zu führen. [52]). Dies ist jedoch im Einzelfall anwaltlich zu prüfen [52].

4.1.4 Informationssicherheitsteam

Das Informationssicherheitsteam besteht aus den Vertretungen der drei großen Säulen (Abbildung 7: Organigramm eines Informationssicherheitsteam) der Informationssicherheit in einem Unternehmen:

- Datenschutz/-sicherheit
  Der Datenschutz/die Datensicherheit wird meist durch den/die Datenschutzmanager(in) oder die/den Datenschutzbeauftragte(n), sofern diese Position besetzt ist, vertreten.
- Geschäftsleitung
- Belegschaft
  Die Belegschaft ist neben einem/einer IT-Verantwortlichen auch mit Vertretern/Vertreterinnen der Mitarbeitenden im IST vertreten. Wenn in einem Unternehmen ein Betriebsrat vorhanden ist, so kann ein(e) Vertreter(in) des Betriebsrates die Vertretung der Mitarbeitenden übernehmen.

Den Vorsitz des Informationssicherheitsteams hat die informationssicherheitsbeauftragte Person inne, die ebenfalls Teil des IST ist und von der Geschäftsleitung bestimmt wird.

Die Hauptaufgabe eines/einer Informationssicherheitsbeauftragten ist die Erreichung der – durch die Informationssicherheitsrichtlinien des Unternehmens – festgelegten Ziele. Zudem ist der/die ISB für die Implementierung dieser Richtlinien zuständig. Hierzu gehören das Steuern, Koordinieren und Prüfen von existierenden und das Planen von neuen Maßnahmen, um die Informationssicherheit an die Bedrohungen und Änderungen im Umfeld des Unternehmens und an neue gesetzliche, betriebliche und vertragliche Anforderungen anzupassen.

Damit auch bei Abwesenheit einzelner Mitglieder des IST die Verantwortlichkeiten im Bereich der IT-Sicherheit wahrgenommen werden können, ist es ratsam, Vertretungen zu regeln.

4.2 Leitlinie zur Informationssicherheit

Eine Leitlinie zur Informationssicherheit dient als das zentrale Dokument für die gesamte Informationssicherheit eines Unternehmens. Der/Die ISB erstellt diese Leitlinie mithilfe des IST und die Geschäftsleitung setzt diese in Kraft. Die Geschäftsleitung ist verpflichtet, diese Leitlinie jährlich zu prüfen und ggf. anzupassen bzw. durch den/die ISB und das IST anpassen zu lassen, wenn das Unternehmen sich zertifizieren lässt.

In der Leitlinie sind die von der Geschäftsleitung vorgegebenen Ziele und sämtliche Verantwortlichkeiten definiert. Weiterhin müssen gemäß der VdS Richtlinien individuelle Konsequenzen bei Zuwiderhandeln gegen die Leitlinie festgelegt werden.

Jede Änderung der Leitlinie sowie eine Neuerstellung dieser müssen jeder Zielgruppe in verständlicher Form zugänglich gemacht werden.

4.3 Richtlinien zur Informationssicherheit

Genauso wie die Leitlinie zur Informationssicherheit eines Unternehmens wird auch jede Richtlinie in der Informationssicherheit des Unternehmens von dem/der ISB mit Unterstützung des IST erstellt. Die Geschäftsleitung muss diese ebenfalls freigeben. Bei der Erstellung der Richtlinien sollte der/die ISB die gesetzlichen, vertraglich vereinbarten und behördlichen Anforderungen ermitteln und in die Erstellung der Richtlinien integrieren.

Jede Änderung ist – wie bei der Leitlinie – unverzüglich zielgruppenspezifisch (ggf. durch eine Mitarbeitenden-Schulung) bekannt zu machen. Mit jeder Richtlinie müssen laut den Richtlinien der VdS folgende Anforderungen erfüllt werden:

- Die Zielgruppe, für die dieses Dokument verbindlich ist, muss enthalten sein.
- Grund und Zweck der Erstellung
- Ein Verstoß dieser Richtlinie gegen andere interne sowie externe Richtlinien kann ausgeschlossen werden.
- In der Richtlinie ist ein Hinweis auf die Konsequenzen bei Nichtbeachtung enthalten.

Bei der Erstellung einer Richtlinie sind Regeln insbesondere in Bezug auf Verhalten, Missbrauch und Nutzung fest zu definieren (vgl. Kapitel 6.3 oder Seite 16 VdS 10000). Weitere themenspezifischere Regelungen sind im Bedarfsfall zu erarbeiten und zu integrieren (vgl. 6.4 VdS 10000).

4.4 Mitarbeitende

Mitarbeitende eines Unternehmens sind für die Implementierung und Aufrechterhaltung der Informationssicherheit von entscheidender Bedeutung.

Bei den Mitarbeitenden wird in der VdS 10000 [26] zwischen drei Gruppen unterschieden:

- Mitarbeitende vor Aufnahme der Tätigkeit
- Mitarbeitende bei Ausübung der Tätigkeit
- Mitarbeitende nach Beendigung der Tätigkeit

Für die erste Gruppe muss ein Unternehmen sicherstellen, dass zukünftige Mitarbeitende keine potentielle Gefährdung darstellen, für die Ausübung der Tätigkeit geeignet und generell vertrauenswürdig sind.

Während Mitarbeitende im Unternehmen tätig sind, müssen diese sich gemäß den Richtlinien der VdS schriftlich mit den Aufgaben und Pflichten und der Informationssicherheitsleitlinie einverstanden erklären. Das Unternehmen muss dafür Sorge tragen, dass neues und bestehendes Personal bei Bedarf zeitnah in sämtlichen entsprechenden Reglungen, Verfahren und Sicherheitsmaßnahmen unterwiesen wird.

Für die Ausübung ihrer Tätigkeit erhalten die Mitarbeitenden während der Tätigkeit alle erforderlichen Zugänge, Zugriffsrechte und IT-Ressourcen und werden in der sicherheitsorientierten Nutzung geschult.

Für die Sicherstellung der erfolgreichen und vollumfänglichen Beendigung eins Beschäftigungsverhältnisses zwischen Mitarbeitenden und dem Unternehmen muss ein Verfahren implementiert werden. Hierin wird geregelt, welche Stellen über diese Personalmaßnahme informiert und welche Daten und Ressourcen (bspw. IT-Ressourcen, Zugänge und Zugriffsrechte) wieder entfernt bzw. zurückgegeben werden müssen.

Die oben beschriebenen Regelungen für Mitarbeitende gelten im Wesentlichen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine, kleine als auch mittlere Unternehmen.

4.5 Wissen

Dadurch, dass vielen Personen Risiken und Gefahren in der Informationssicherheit oftmals nicht bewusst sind bzw. sie diese nicht kennen, entstehen vermehrt Gefährdungen. Um diese Gefährdungen zu minimieren, ist es notwendig, den Personen das Wissen darüber zu vermitteln bzw. bereitzustellen. Hierfür sind in einem Unternehmen Prozesse zu integrieren, damit sämtlichen Mitarbeitenden und relevanten Personengruppen neue und geänderte Informationen zeitnah zur Verfügung gestellt und vermittelt werden. Weiterhin ist sicherzustellen, dass in regelmäßigen Abständen auch an bestehende Informationen erinnert wird. Dieses Verfahren muss gemäß der Richtlinie VdS 10000 [26] sicherstellen, dass in regelmäßigen Abständen Informationen über die aktuellen technischen und rechtlichen Veränderungen in der Informationssicherheit von vertrauenswürdigen Quellen bezogen, ausgewertet und an die betreffenden Personenkreise verteilt wird. Hierbei empfiehlt es sich, dass die Verantwortlichen der IT-Sicherheit Kontakt zu Sicherheitsforen und Interessengruppen halten, um sich mit den Fachkräften anderer Unternehmen auszutauschen und auf dem aktuellen Wissenstand bleiben zu können.

Für die Wissensvermittlung von IT-Sicherheitsverantwortlichen an Mitarbeitende des Unternehmens ist ein Verfahren, das die Mitarbeitenden regelmäßig und bedarfsgerecht über Änderungen informiert und sensibilisiert, zu implementieren.

In den Schulungen wird den Teilnehmenden der Umgang mit den internen Sicherheitsmaßnahmen, das Verhalten bei Störungen, Ausfällen und Sicherheitsvorfällen erklärt sowie die Akzeptanz für diese Maßnahmen erzielt. Mit dem Verfahren geht eine Dokumentation der vermittelten Inhalte und der Teilnehmenden einher. Eine Wissensabfrage bzw. eine Lernkontrolle sollte ebenfalls Teil einer jeden Schulung sein.

Dieses Kapitel ist nicht Bestandteil der VdS 10005 [27] und daher insbesondere für sehr kleine Unternehmen nicht vorgesehen.

4.6 Identifizieren kritischer IT-Ressourcen

Der/Die ISB ist für die jährliche Überprüfung und etwaige Anpassung der IT-Ressourcen – insbesondere der kritischen IT-Ressourcen – zuständig.

Dem/Der ISB stehen hierfür verschiedene Standard-Methoden zur Verfügung:

- Informationsklassifizierung basierend auf dem aktuellen ISO/IEC-Standard 27001 (siehe 3.2)
- Schutzbedarfsanalyse basierend auf dem aktuellen BSI Standard 200-2 (siehe 2.3.1.2)

Wird eine andere Methode gewählt, muss diese gemäß der Richtlinie VdS 10000 für eine Zertifizierung die gleichen Anforderungen erfüllen und genauestens dokumentiert werden.

Dieses Kapitel ist nicht Bestandteil der VdS 10005 und daher für kleine und insbesondere für sehr kleine Unternehmen nicht vorgesehen.

4.7 IT-Systeme

In den meisten Unternehmen geschieht die Verarbeitung von Informationen wie den Kundendaten oder Bankdaten größtenteils in elektronischer Form. Genauso wie analoge Medien gegen beispielsweise Diebstahl im Tresor verwaltet oder gegen Verlust im Ordner strukturiert abgeheftet werden, muss dies in gleichem Maße auch bei digitalen Medien geschehen.

Hierfür ist es dringend notwendig, die IT-Systeme zu inventarisieren und gegen Gefahren abzusichern.

Bei der Inventarisierung muss gemäß der Richtlinie VdS 10000 jedem IT-System ein eindeutiges Merkmal zur Identifizierung (z. B. mit einem Zahlencode), ein Einsatzzweck und eine Information, die den genauen Standort des Systems beinhaltet, zugewiesen werden. Weitere Informationen wie die Lizenzinformationen bei Software oder die Seriennummer bei Hardware sind hilfreich, um die Aktualisierung der Systeme zu vereinfachen.

All diese Informationen und Besonderheiten bei der Installation und Wartung der IT-Systeme sollten genauestens dokumentiert werden.

4.7.1 Lebenszyklus

Ähnlich wie bei den Mitarbeitenden (Kapitel 4.4) müssen bei Hard- und Software Verfahren in die IT-Sicherheit eines Unternehmens integriert werden, die den verantwortungsbewussten Umgang vor, während und nach dem Betrieb des IT-Systems sicherstellen.

Vor der Inbetriebnahme und während des Betriebs eines (neuen) IT-Systems müssen vier Anforderungen erfüllt werden:

- Überprüfung, ob das (neue) System ein oder ein Teil eines kritischen IT-Systems ist. (4.6)

- Erfüllung der Anforderungen an den Basisschutz (siehe 4.7.2) des (neuen) Systems
- Erweiterung der Inventarisierung um die Informationen des (neuen) IT-Systems
- Dokumentation aller Arbeitsschritte.

Hat ein IT-System das Ende seines Lebenszyklusses erreicht und wird ausgemustert oder an anderer Stelle wiederverwendet, müssen gemäß den VdS Richtlinien VdS 10000 und VdS 10005 neben der Dokumentation verschiedene Schritte zur Wahrung der Informationssicherheit erfolgen.

Alle Informationen, die auf dem auszumusternden IT-System vorhanden bzw. mit diesem verbunden sind, müssen bei Bedarf gesichert und zuverlässig gelöscht, überschrieben oder durch Zerstörung der Hardware vernichtet werden, sodass kein unberechtigter Zugriff auf diese Daten erfolgen kann. Dies impliziert auch die Löschung des IT-Systems aus der Inventarisierung und dem Netzwerkplan (4.8) des Unternehmens.

4.7.2 Basisschutz

Der Basisschutz definiert einen grundlegenden Schutz, der für sämtliche IT-Systeme in einem Unternehmensnetzwerk verpflichtende Vorgaben macht.

Im Folgenden werden die Bestandteile des Basisschutzes kategorisiert betrachtet:

Jede Software, die im Unternehmensnetzwerk verwendet wird, darf nur aus vertrauenswürdigen Quellen bezogen werden, um die Gefahr von potentieller Schadsoftware so gering wie möglich zu halten und sollte dazu stets auf dem aktuellsten Stand sein. Eine vertrauenswürdige Quelle ist die Herstellerseite. Werden Programme von Drittanbietern zum Kauf oder Download angeboten, ist dies immer mit Vorsicht zu betrachten.

Grundsätzlich wird empfohlen, Software nur aus vertrauenswürdigen Quellen (bspw. direkt vom Hersteller oder einem autorisierten Händler) zu beschaffen.

Zusätzlich sollte lediglich für die Beschäftigung relevante Software installiert sein. Software, die nicht zur Erledigung von Tätigkeiten eines Unternehmens dient, sollte deinstalliert werden.

Genauso wie Software, die nicht genutzt und benötigt wird, sollten auch externe Schnittstellen wie Laufwerke oder USB-Ports deaktiviert, reduziert bzw. mechanisch blockiert werden, sodass sie für die Anwendenden nicht zugänglich sind.

Der überwiegende Teil der Unternehmen besitzt Netzwerke, die mit dem Internet verbunden sind. Für alle aber gilt, den Netzwerkverkehr auf ein Minimum zu beschränken, da Unternehmensnetzwerke sehr exponiert sind und dadurch die Wahrscheinlichkeit einer Schwachstellenausnutzung deutlich höher ist.

Möglich gemacht werden kann dies durch Filtermechanismen (bspw. eine Firewall) zwischen den Netzwerken oder durch das Deaktivieren von ungenutzten Programmen.

Zum Basisschutz gehört auch ein Verfahren zur Dokumentation. Bei dieser Protokollierung werden z. B. Daten in Zusammenhang mit einem Anmeldeprozess gespeichert. Es wird nur

protokolliert, ob der Anmeldeversuch erfolgreich oder -los geschieht. Diese und andere nicht personenbezogenen Informationen sollten zentral gespeichert und müssen für ein halbes Jahr gesichert werden [26].

Für alle Systeme im Unternehmensnetzwerk sind präventive Maßnahmen wie der Schutz vor Schadsoftware verpflichtend. Bei Systemen ohne einen Echtzeitschutz ist dieser Schutzstatus täglich zu überprüfen, bei Systemen mit Echtzeitschutz übernimmt diese Aufgabe primär die Echtzeitkomponente und die Überprüfung muss nur wöchentlich erfolgen.

Die VdS Schadensverhütung rät dazu, den nicht verpflichtenden Echtzeitschutz zu aktivieren.

Eine weitere Komponente des Basisschutzes ist die Sicherstellung, dass IT-Systeme nur von autorisierten Medien gestartet werden können. Durch diese Maßnahme sollen wichtige Sicherheitsmaßnahmen wie Zugriffsbeschränkungen gewährleistet oder das System vor Schadsoftware geschützt werden [53].

Damit ein IT-System den Basisschutz erhält, müssen neben den eben erläuterten Aspekten auch die Authentifizierungsmechanismen und die Zugänge und Zugriffe kontrolliert werden. Dafür ist es essentiell, dass der interne gegenüber dem externen Bereich durch geeignete Verfahren abgesichert wird.

- Sichere Passwörter bzw. zuverlässige Authentifizierungsmaßnahmen sind in sämtlichen Bereichen des IT-Systems verpflichtend (neue Passwörter dürfen den alten nicht ähneln). Triviale Passwörter oder die Standardpasswörter, die über die Werkseinstellung von Herstellern in den IT-Komponenten implementiert sind, dürfen im Basisschutz nicht verwendet und müssen vorab geändert werden.
- Ist ein/eine Nutzer/Nutzerin inaktiv, so wird der Zugang nach einer vorher definierten Zeitspanne gesperrt und der Zugriff muss erneut verifiziert werden.
- Erfolgt der Zugriff über ein Netzwerk, müssen Vertraulichkeit und Integrität durch entsprechende Sicherheitsprotokolle sichergestellt werden.

Jeder einzelne Zugang muss strukturiert verwaltet werden (vgl. 4.12). Bei besonderen Zugängen oder mit besonders hohen oder speziellen Zugriffsrechten sollte eine mehrfache Authentifizierung erfolgen (vgl. Mehr-Faktor-Authentifizierung), um den Zugang für Unbefugte zu erschweren. Es muss sichergestellt werden, dass Standard-Nutzende keine administrativen Zugriffsrechte besitzen und lediglich Lese- und Schreibrechte für Bereiche, die zur Erfüllung ihrer Aufgaben erforderlich sind, erhalten (vgl. „Need-to-know“ und „Least-Privileges“).

4.7.3 Maßnahmen bei mobilen Systemen im Unternehmensnetzwerk

Im Umgang mit mobilen Systemen und Datenträgern (vgl. Kapitel 12 in der VdS 10000) ist besondere Vorsicht geboten, da diese in Bezug auf Diebstahl und unautorisierte Zugriffe besonders stark gefährdet sind bzw. Gefährdungen für das Unternehmensnetzwerk darstellen. Für die Nutzung von mobilen Systemen sind folgende Aspekte verpflichtend:

- Dokumentation aller erhobenen, verarbeiteten, gespeicherten und übertragenen Daten
- Festlegung der Verantwortlichkeiten für die Datensicherung

- Sensibilisierung und Aufklärung der Mitarbeitenden in Bezug auf die Risiken im Umgang mit mobilen Systemen und dementsprechendes Handeln
- Festlegung der Szenarien, in denen eine administrierende Person ein mobiles System orten und/oder Daten aus der Ferne löschen oder verändern darf (bspw. bei Verlust)
- Verschlüsselung der Datenträger von mobilen Systemen, um die Vertraulichkeit und Integrität der Daten zu schützen (bspw. bei Verlust)
- Festlegung von Verfahren, die bei einem Verlust eines mobilen Systems die Vorgehensweise beschreiben (Meldepflichten, Sofortreaktionen)

4.7.4 Maßnahmen bei kritischen Systemen im Unternehmensnetzwerk

Neben den mobilen Systemen müssen für die kritischen IT-Systeme (bspw. Steuerung der Gepäckabfertigung am Flughafens, Lüftung in einem Serverraum) zusätzliche Maßnahmen umgesetzt werden. Für jedes kritische System ist eine Risikoanalyse und entsprechende -behandlung unabdingbar.

Kritische IT-Systeme sind dem Namen zufolge kritisch für die IT-Sicherheit des Unternehmensnetzwerkes und sollten daher mit einem „Notbetriebsniveau“ abgesichert werden. Aufgrund der kritischen Aspekte des IT-Systems dürfen auf diesem keine Tests oder Entwicklungen stattfinden. Jegliche Updates müssen erst auf ähnlichen Systemen getestet und dürfen erst nach erfolgreichem Test auf das kritische IT-System übertragen werden.

Wie in Kapitel 4.7.2 beschrieben dürfen auf kritischen Systemen keine ungenutzten Zugänge (freie Ports, Laufwerke, etc.) zur freien Benutzung stehen und nicht erforderliche Software (vorinstallierte Spiele, Media-Player, etc.) muss deinstalliert werden, wenn diese nicht der Aufgabenerfüllung dient. Ein kritisches System muss verpflichtend über eine Datensicherung und eine Überwachung verfügen. Bei der Überwachung muss sichergestellt sein, dass ein Ausfall erkannt werden kann und dementsprechende Maßnahmen schnellstmöglich eingeleitet werden. Neben einer Datensicherung für ein kritisches IT-System muss ein Unternehmen über ein redundantes Ausweichsystem verfügen, damit bei einem Ausfall und nicht erfolgreicher Wiederherstellung (Nichteinhaltung der vorher definierten maximal tolerierbaren Ausfallzeit (MTA)) der Betrieb fortgesetzt werden kann. Bei kritischen IT-Systemen muss gemäß den VdS Richtlinien sichergestellt werden, dass die Software auch in Zukunft bereitgestellt wird. Im Zweifelsfall muss durch vertragliche Vereinbarungen eine Ersatzsoftware zugesichert werden. Die oben beschriebenen Regelungen für IT-Systeme gelten im Wesentlichen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine, kleine als auch mittlere Unternehmen.

4.8 Netzwerke und Verbindungen

Jedes Unternehmen muss bei einer Zertifizierung einen Netzwerkplan vorlegen, mit dem fachlich versierte Personen die physikalischen und logischen Strukturen des Unternehmens nachvollziehen können.
Für die Kommunikation zwischen Netzwerken gilt, dass diese auf das Minimum zu beschränken ist. Über Netzwerkübergänge laufende Schadsoftware oder Angriffe müssen zuverlässig analysiert und blockiert werden. Jeder Angriff muss als Sicherheitsvorfall angesehen und entsprechend behandelt werden. Die Kommunikationseinstellungen von internen zu externen Netzwerken (und umgekehrt) muss jährlich überprüft und ggf. angepasst werden.
Wie bei den IT-Systemen gibt es auch bei den Netzwerken eine Art Basisschutz. Dieser schreibt gemäß der VdS Richtlinien vor, dass…

- Sämtliche nicht genutzte Netzwerkanschlüsse vor unberechtigtem Zugriff gesichert werden müssen.
- Das IT-System des Unternehmens wenn möglich in kleinere Netzwerke segmentiert werden sollte (sehr kleinen und kleinen Unternehmen fehlen meist die Möglichkeiten dafür). Geschieht dies nicht, muss dies ebenfalls protokolliert werden.
- Ein Fernzugang abgesichert werden muss. Fernzugänge sind so zu konfigurieren, dass nur die minimal nötige Kommunikation gemäß der Aufgabenerfüllung möglich ist. Die Schutzziele Vertraulichkeit, Integrität und Authentizität sind zu wahren.
- Sichergestellt werden sollte, dass besondere Zugriffsrechte durch zusätzliche Authentifizierungsmaßnahmen (z. B. Mehrfachauthentifizierung) gesichert werden.
- Netzwerkkopplungen auf ein Minimum beschränkt und gegenüber weniger vertrauenswürdigen Netzwerken abgesichert werden.
- Im Falle einer kritischen Verbindung eine Risikoanalyse verpflichtend ist.

Die oben beschriebenen Regelungen für Netzwerke und Verbindungen gelten bis auf wenige Ausnahmen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine und kleine als auch mittlere Unternehmen. Bspw. ist eine Segmentierung des Unternehmensnetzwerk bei sehr kleinen Unternehmen oftmals nicht möglich.

4.9 Mobile Datenträger

Die Inhalte dieses Kapitels wurden in Kapitel 4.7.3 erklärt.

Dieses Kapitel ist nicht Bestandteil der VdS 10005 und daher für kleine und insbesondere für sehr kleine Unternehmen nicht vorgesehen.

4.10 Umgebung

Die IT-Systeme und Datenleitungen müssen nicht nur gegen Angriffe, sondern auch gegen äußere Umwelteinflüsse wie Wasser, Feuer oder Wind geschützt werden. Anerkannte Standards wie die VdS 2007 [54] helfen bei der Umsetzung.

Dies gilt bis auf wenige Ausnahmen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine und kleine als auch mittlere Unternehmen.

4.11 IT-Outsourcing und Cloud-Computing

Beim Auslagern von IT-Systemen, -Ressourcen und/oder -Dienstleistungen müssen zuerst die Unternehmensinteressen gewahrt werden. Weiterhin muss jede Auslagerung begründet und dokumentiert werden. Die Auslagerung darf nicht gegen andere vertragliche, betriebliche oder gesetzliche Vorschriften verstoßen. Das anbietende Unternehmen, an das ausgelagert wird, muss vertraglich dazu verpflichtet werden, in Bezug auf die unternehmensbezogenen Daten die Informationssicherheitsrichtlinien des Unternehmens einzuhalten bzw. zu befolgen.

Die oben beschriebenen Regelungen für das IT-Outsourcing und Cloud-Computing gelten im Wesentlichen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine und kleine als auch mittlere Unternehmen.

4.12 Zugänge und Zugriffsrechte

Durch Zugänge und Zugriffsrechte ist es möglich, den Zugriff auf interne Daten und Strukturen eines Unternehmens zu steuern. Daher müssen die Informationen zu den Zugängen und Zugriffsrechten sicher und strukturiert verwaltet werden.

Das Unternehmen muss ein Verfahren entwickeln, mit dem Zugänge und Zugriffsrechte hinzugefügt, verändert und entfernt werden können. Administrative Zugänge und Rechte werden nur nach ausführlicher Begründung und in Abstimmung mit dem ITV vergeben.

Wird ein Zugang entfernt, werden alle dazugehörigen Daten gesichert, ggf. weitergegeben oder archiviert. Jeder Vorgang muss dokumentiert werden.

Die oben beschriebenen Regelungen für die Verwaltung von Zugängen und Zugriffsrechten gelten im Wesentlichen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine, kleine als auch mittlere Unternehmen.

4.13 Datensicherung und -archivierung

Durch einen Angriff oder andere Einflüsse können Daten unbrauchbar werden. Um das Unternehmen durch den Verlust dieser Daten nicht zu behindern, sind Datensicherungen von entscheidender Bedeutung.

Eine Datensicherung kann mit dem BSI-Standard 200-2 erfolgen. In diesem sind alle Anforderungen an die Datensicherheit aus der VdS 10000 enthalten.

Diese Regelungen für die Datensicherung und -archivierung gelten im Wesentlichen laut den VdS Richtlinien VdS 10000 und VdS 10005 sowohl für sehr kleine, kleine als auch mittlere Unternehmen.

Viele der Daten und Informationen, die bei kleinen und mittleren Unternehmen gesichert werden müssen, existieren insbesondere bei sehr kleinen Unternehmen aufgrund der Größe des Unternehmens nicht.

4.14 Störungen und Ausfälle

Störungen und Ausfälle behindern den reibungslosen Betriebsablauf eines Unternehmens. Um diesen schnell wiederherzustellen, ist eine angemessene Reaktion in einer angemessenen Zeit notwendig. Dafür eignen sich insbesondere für sehr kleine Unternehmen, aber auch für kleine und mittlere Unternehmen, vorher definierte Wiederanlaufpläne, in denen das genaue Vorgehen detailliert beschrieben wird. Das Unternehmen ist angehalten, ein sog. Business-Continuity-Management auf der Basis des neuen BSI-Standards 200-4 (bis zur finalen Veröffentlichung des aktualisierten Standards BSI 200-4, gilt weiterhin der BSI 100-4) zu implementieren. Dieses Kapitel ist nicht Bestandteil der VdS 10005 und daher für kleine und insbesondere für sehr kleine Unternehmen nicht vorgesehen.

4.15 Sicherheitsvorfälle

In den vorherigen Kapiteln wurde häufig beschrieben, dass ein unvorhergesehenes Ereignis als ein Sicherheitsvorfall behandelt werden muss. Auf diese Sicherheitsvorfälle sollte im Sinne der Unternehmenssicherheit und des reibungslosen Betriebsablaufes angemessen reagiert werden. Hierzu muss der Begriff des Sicherheitsvorfalls klar definiert und jedem Stakeholder/Stakeholderinnen des Unternehmens mitgeteilt werden.

Mögliche Sicherheitsvorfälle sind immer auch dem/der Informationssicherheitsbeauftragten (und ggf. der Geschäftsleitung) zu melden. Er/Sie ist im Folgenden für die Untersuchung und die Behebung des Problems zuständig. Bestenfalls werden alle Angriffe, bevor diese Schaden anrichten können, erkannt. Um diesen Zustand ermöglichen zu können, sind Maßnahmen wie das Implementieren von Intrusion-Detection-Systemen (IDS), Integritätsprüfungen im Datenverkehr, irreführende Locksysteme (Honey-Pots), besondere Überwachungsmechanismen für besonders sensible Daten und das Erfassen und Auswerten von Log-Daten zu implementieren [26, S. 38].

Kommt es trotz aller Maßnahmen und Vorkehrungen dennoch zu einem erfolgreichen Angriff, ist im ersten Augenblick Ruhe zu bewahren und das Gewinnen einer Übersicht von entscheidender Bedeutung. Besteht keine akute Gefahr für Leib und Leben, können Sofortmaßnahmen bzgl. der Eindämmung des Schadens getroffen werden – andernfalls werden alle erforderlichen Maßnahmen getroffen, um in Gefahr schwebende Personen aus dem Gefahrenbereich (z. B. überhitzende Maschinen, unkontrolliert laufende Turbinen) zu evakuieren.

Für spätere Ansprüche gegenüber Versicherungen sollten alle getroffenen Maßnahmen dokumentiert und Beweismittel gesichert werden. Die Beweismittel sind auch für die Strafverfolgung relevant. Zuletzt wird der Regelbetrieb des Betriebsablaufes wiederhergestellt und der Sicherheitsvorfall im Nachhinein analysiert, um die Ursachen zu ermitteln und geeignete Verbesserungen für die Zukunft zu erarbeiten.

Dieses Kapitel ist nicht Bestandteil der VdS 10005 und daher für kleine und insbesondere für sehr kleine Unternehmen nicht vorgesehen.

4.16 Zusammenfassung

Auf der Basis der beiden Richtlinien VdS 10000 [26] und VdS 10005 [27] wurden in diesem Kapitel die relevanten Anforderungen zur Implementierung eines ISMS bei KMU beschrieben.

5 Grundzüge eines Leitfadens

In diesem Kapitel werden die grundlegenden Eigenschaften und der Aufbau eines Leitfadens im Allgemeinen erläutert. Im nächsten Kapitel (Kapitel 6) wird auf dieser Grundlage der spezielle Leitfaden für die Implementierung eines ISMS bei KMU dargestellt.

Leitfäden sind Handlungsvorschriften. Im Allgemeinen werden hierin Handlungsanweisungen für den jeweiligen Adressaten verständlich formuliert. Diese müssen für die Adressaten des Leitfadens übersichtlich, strukturiert und verständlich dargestellt werden, sodass sie sich mithilfe eines Leitfadens in einer unbekannten Materie besser orientieren können und sich daher besser in einer entsprechenden Situation zurechtfinden [55]. Ein Leitfaden verpflichtet seine Adressaten nicht, kann aber einen leicht bindenden Charakter haben. Ein Leitfaden ist daher eher eine Orientierungshilfe, die Laien erklärt, wie sie mit bestimmten neuartigen Thematiken umgehen sollten [10].

Leitfäden gibt es in allen Berufen zu den unterschiedlichsten Themengebieten und auch im privaten Bereich. Beispielsweise haben die Bundesländer in der Corona-Pandemie Vorschriften und Richtlinien zum Schutz der Bevölkerung und zur Verhinderung der Ausbreitung des Virus herausgebracht, die für viele Bürgerinnen und Bürger meist unverständlich waren, da diese rechtssicher formuliert werden mussten. Um der Bevölkerung die Vorschriften und Handlungsanweisungen näher zu bringen bzw. verständlich zu machen, wurden Leitfäden zur Bekämpfung des Corona-Virus (Abstandsregeln, Hygienevorschriften, Tragen von Masken) in einfacher und eindeutiger Sprache entwickelt [56]. Diese Leitfäden wurden in sehr einfacher Sprache oder mithilfe von Piktogrammen verfasst, damit alle Bevölkerungsgruppen die Vorschriften und Richtlinien „lesen“ und sich dementsprechend verhalten konnten.

Weitere Beispiele für Leitfäden:

- Verhalten bei Vorgaben zur Produkt-Reklamation durch einen Kunden/eine Kundin (Was müssen die Mitarbeitenden tun, wenn jemand ein Produkt reklamieren möchte?)
- Vorgaben zur Vereinheitlichung beim Verfassen einer wissenschaftlichen Arbeit (Formatierungen, Zitation, …)
- Bildliche Beschreibung der Benutzung der Toilette für Kinder im Kindergarten (Händewaschen, Deckel schließen, Licht aus, …)
- Aufzeigen von falschen Verhaltensweisen im Umgang mit Mitarbeitenden (Mobbing am Arbeitsplatz oder Cybermobbing)

Je nach Zielgruppe muss ein Leitfaden unterschiedlich aufgebaut sein. Wird beispielsweise ein Leitfaden für Kinder im Kindergarten für die Benutzung der Toilette erstellt, sollte dies kinderfreundlich mit vielen Bildern geschehen, da Kinder in dem Alter meist noch keine Schrift lesen können.

Bei Erwachsenen, die bspw. für die Produktreklamation zuständig sind, ist dies zur Erstellung eines Leitfadens nicht erforderlich. Je nach Ausrichtung des Leitfadens ist aber auch hier eine situationsangepasste Sprache mit Piktogrammen und/oder Schaubildern verständlicher. Leitfäden sind situationsabhängig aufgebaut und haben keinen allgemeingültigen Aufbau. Je nach

Aufgabengebiet gibt es bei Leitfäden große Unterschiede in Aufbau und Umfang [10]. Jedoch sind in jedem Leitfaden einige Aspekte standardmäßig enthalten bzw. sollten enthalten sein [10].

- Jeder Leitfaden hat einen aussagekräftigen **Titel**.
- Eine auf die Zielgruppe bezogene Erklärung erfolgt am Anfang des Leitfadens, die den Inhalt des Leitfadens beschreibt, um einen genaueren **Einblick in die Thematik** zu vermitteln.
- Im Folgenden sollten die angesprochenen **Zielgruppen** beschrieben werden. Hierbei sollte darauf geachtet werden, dass der Leitfaden so gestaltet wird, dass die Zielgruppen über das nötige Wissen verfügen, die neuen Kompetenzen zu erlernen oder sich das dafür notwendige Wissen aneignen zu können.
- Der Hauptteil des Leitfadens sollte in sinnvolle Abschnitte eingeteilt werden. In jedem Abschnitt werden die **Handlungsanweisungen** aufgeführt und mittels **Fragestellungen** und **Lösungsvorschlägen** ausgeführt.
- Zum Schluss erfolgt eine **Zusammenfassung** des Leitfadens.
- Der **Zeitpunkt der Erstellung** sowie die **Verantwortlichkeiten** werden auf einer separaten Seite vermerkt (z. B. Impressum oder Versionshistorie).

Leitfäden können, da diese nicht genormt sind und somit frei gestaltet werden können, jede situationsangepasste Struktur erhalten.

Ein Beispiel für eine solche Struktur ist ein Ablaufplan.

- **Wenn** …, **dann** …:
  Diese Struktur ermöglicht es, Abläufe in einem Leitfaden zu beschreiben. (**Wenn** der Nutzende den Strom abschaltet, **dann** kann er die ehemals stromführenden Leitungen gefahrlos berühren.)

6 Erstellung des Leitfadens für die Einführung eines ISMS bei KMU

In Kapitel 5 wurde beschrieben, wie Leitfäden im Allgemeinen aufgebaut sind. In diesem Kapitel wird das eigentliche Ziel dieser Arbeit – die Erstellung eines Leitfadens zur Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen – detailliert erläutert.

Der in sich abgeschlossene Leitfaden für die Einführung eines Informationssicherheitsmanagementsystems in kleinen und mittleren Unternehmen ist der Arbeit als Anhang A angefügt.

Nachfolgend werden die folgenden Fragen beantwortet:

- Welche Ziele soll der Leitfaden erfüllen?
- An wen richtet sich dieser Leitfaden bzw. welche Zielgruppen sollen durch den Leitfaden angesprochen werden?
- Welche Struktur wurde bei diesem Leitfaden gewählt?

6.1 Zielsetzung des Leitfadens

Die Sicherheit von Informationen wird im Alltag von kleinen und mittleren Unternehmen immer wichtiger. Die Kommunikation wechselt vom Brief zur E-Mail, der Datenaustausch vom Kurier zum Server oder allgemeiner formuliert: Unternehmen digitalisieren sich, damit sie wettbewerbsfähig bleiben.

Dabei sind die Gefahren der Digitalisierung ähnlich zu den analoger Vorgehensweisen.

- Das illegale Abfangen, Öffnen und Mitlesen von E-Mails ist analog zum unrechtmäßigen Abfangen, Öffnen und Mitlesen eines Briefes zu sehen. Brief- und Fernmeldegeheimnis [57] (Telekommunikationsgeheimnis Art. 73 Nr. 7 GG [58]) sind im Grundgesetz der Bundesrepublik Deutschland verankert und stellen Grundrechte dar.
- Der Diebstahl von Kuriersendungen ist digital ebenfalls möglich, indem Datenpakete auf einem Server abgefangen oder ausgelesen werden, während im analogen Bereich Pakete physisch abgefangen werden.
- Das Abschließen der Türen nach Geschäftsschluss ist vergleichbar mit dem Abmelden und Herunterfahren der Computer im Unternehmen.

Dies sind nur drei Beispiele, die veranschaulichen, dass die Gefahren vergleichbar sind.

KMU müssen sich daher der Digitalisierung und den damit einhergehenden Risiken stellen und sich mit diesen neuen Gefahren auseinandersetzen, obgleich dadurch die bisher bekannten Risiken nicht außer Acht gelassen werden dürfen. Viele Unternehmen dürften jedoch das Problem haben, dass sie nicht über das nötige Wissen für die Auseinandersetzung mit den neuen Gefahren verfügen oder wenig Affinität zum Thema Informationstechnik besitzen. Hintergrund könnte sein, dass die Technik ein Mittel zum Zweck, aber nicht die unmittelbare Hauptaufgabe des Unternehmens ist. Für viele Nutzende scheint die digitale Welt im Berufsleben noch immer unbekanntes Terrain zu sein.

Außerdem scheint es so, dass sowohl die Mitarbeitenden als auch viele Führungskräfte bisher ein geringes Problembewusstsein in Bezug auf die Informationstechnik entwickelt haben bzw. besitzen. Oft werden z. B. immer noch einfach zu merkende Passwörter gewählt, da sie den Wert ihrer Daten für Cyberkriminelle nicht erkennen und einen Angriff auf das eigene Unternehmen als unwahrscheinlich ansehen. Die auf der Unkenntnis oder Fehleinschätzung basierenden niedrigen Sicherheitsvorkehrungen im digitalen Bereich nutzen jedoch Cyberkriminelle als Schwachstellen, um technisch in das Unternehmen zu gelangen, um z. B. die Systeme zu sperren und das Unternehmen mit Lösegeldforderungen und gleichzeitiger Drohung der Löschung der Daten zu erpressen. Durch diese oder ähnliche Vorgehensweisen wurden in der Vergangenheit viele Systeme (u. a. Stadtverwaltungen) angegriffen und sind dadurch teilweise monatelang ausgefallen ((Stadt) Bad Langensalza [59], (Stadt) Rodgau [60], Continental [61], Enercity [62], Üstra [63], ABB [64], uvm.).

Neben dem Schutz von Daten oder Zugangsberechtigungen, werden mithilfe eines ISMS Verhaltensregeln für diverse Szenarien erstellt und verwaltet.

- Verhaltensregeln über die Nutzung von Hardware (z. B. USB-Ports)
- Verhaltensregeln über die Nutzung von privaten oder unternehmenseigenen Smartphones (bspw. Aufnehmen und Veröffentlichen von Bildern, auf denen im Hintergrund Notizzettel mit Passwörter zu sehen sind, Posten von Bildern auf Instagram zu neuartigen Entwicklungen, Firmengeheimnissen, uvm.)
- Verhaltensregeln zur Vernichtung von Arbeitsunterlagen wie Kunden- und Personaldaten, Krankenakten, geheime Unterlagen (Aktenvernichtung)
- uvm.

Die Informationssicherheit ist dabei nur ein Teil des Aufgabenbereichs von Führungskräften. Damit diese und deren Unternehmen bei der Umsetzung von vorgeschriebenen Maßnahmen unterstützt werden, stellt dieser Leitfaden speziell für die kleinen und mittleren Unternehmen eine aufgearbeitete Anleitung zur Verfügung.

Das Ziel dieses Leitfadens ist, dass kleine und mittlere Unternehmen in der Lage sind, mithilfe dieses Leitfadens erforderliche bzw. notwendige- IT-Sicherheitsmaßnahmen bei der Einführung eines Informationssicherheitsmanagementsystems zu implementieren. Auch wenn eine vollständige Sicherheit vor Cyberangriffen nie gewährleistet werden kann, soll die Wahrscheinlichkeit von erfolgreichen Cyberangriffen gegen KMU bei Umsetzung der Vorgaben dieses Leitfadens sinken bzw. Angriffe idealerweise bereits von Anfang an scheitern lassen.

6.2 Adressaten des Leitfadens

Der Leitfaden richtet sich generell an alle informationssicherheitsinteressierten Personen von kleinen und mittleren Unternehmen. Weil die Verantwortung für Sicherheitsstandards für das jeweilige Unternehmen im Bereich der Führungsebene zu verorten ist, sind die dort tätigen Personen primäre Adressaten für die Nutzung des Leitfadens. Diese werden durch die IT-Verantwortlichen, die Informationssicherheitsbeauftragten und durch die Geschäftsleitung vertreten.

Die genannten primären Adressaten sind für die Verwaltung und Organisation des Unternehmens sowie die Informationssicherheit zuständig. Der Leitfaden ist jedoch so aufgebaut, dass auch Personen ohne besonderes Vorwissen – insbesondere von sehr kleinen Unternehmen – durch alle notwendigen Schritte zur Umsetzung geleitet werden.

6.3 Aufbau des Leitfadens bzw. der Leitfadenstruktur

Wie in Kapitel 5 beschrieben, gibt es verschiedene Ausrichtungen von Leitfäden. Die Adressaten dieses Leitfadens sind die Führungskräfte der Unternehmen mit weniger als 250 Mitarbeitenden. In dieser Personengruppe sind alle Branchen vertreten und besonders die sehr kleinen Unternehmen haben wahrscheinlich bislang wenig Berührungspunkte mit Informationssicherheit, da die digitale Datenverarbeitung nicht ihre Hauptaufgabe darstellt.

Daher versucht dieser Leitfaden, die oftmals in technisch einwandfreier und rechtssicherer Sprache geschriebenen Normen und Richtlinien in verständliche Sprache zu transformieren. Er ist auch kein reiner Text-Leitfaden, sondern besteht aus einer grafischen Übersicht und Erklärungen hierzu.

Damit ein Leitfaden für den Nutzenden ansprechend wirkt, sollte er intuitiv und übersichtlich gestaltet sein. Hierfür wurde eine grafische Übersicht des Leitfadens an den Anfang gesetzt, damit der/die Nutzende sich zunächst einen Überblick verschaffen kann. Diese grafische Übersicht ist in verschiedenen Farben eingefärbt, die einen Farbverlauf ähnlich einer Ampel von Rot (Stop, Gefahr, Aufmerksamkeit und Maßnahmen erforderlich) zu Grün (keine Gefahr, Maßnahmen abgeschlossen, vollständig) beinhalten. Von einer schlechten (roten) Ausgangslage entwickelt sich im Laufe der Abarbeitung (dargestellt durch die Chevron-Pfeile) der Leitlinie ein guter/stabiler Zustand (grün).

Abbildung 8: Grafische Übersicht des Leitfadens

Damit der Leitfaden übersichtlich bleibt, wurden die Erklärungen zu den einzelnen Schritten der grafischen Übersicht in den zugehörigen separaten Kapiteln in farbige Rahmen gesetzt. Dabei wurden die Farben der Übersicht in die Rahmen übernommen. So soll erreicht werden, dass der/die Nutzende zu jeder Zeit erkennen kann, in welchem Schritt des Leitfadens er oder sie sich gerade befindet und gleichzeitig aufzeigen, welcher Fortschritt bislang erzielt wurde.

Damit der Nutzende sich nicht in jedem Schritt neu orientieren muss, wurde im Leitfaden in jedem Schritt der gleiche Aufbau gewählt. Jeder Schritt des Leitfadens wird durch einen farblich hinterlegten Titel, der das Thema des Schritts wiederholt, eingeleitet.

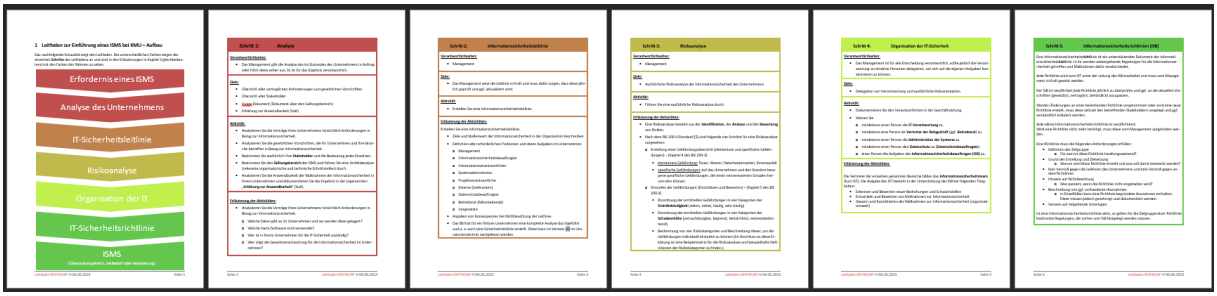

Abbildung 9: Übersicht über die farblich angepassten Rahmen

Einige Schritte sind für sehr kleine Unternehmen mit weniger als zehn Mitarbeitenden nicht vorgeschrieben, sofern das Unternehmen keine Zertifizierung anstrebt. Diese sind durch Fußnoten im Titel gekennzeichnet.

Die Schritte selbst sind in vier Bereiche eingeteilt, um die Orientierung für Nutzende zu erleichtern (siehe Abbildung 10: Aufbau der Schritte des Leitfadens).

Schritt: Titel

Verantwortlichkeiten:

- Hier werden die Verantwortlichkeiten des Vorgangs definiert und ggf. Aufgaben dieser in Bezug auf den Vorgang beschrieben.

Ziele:

- Hier werden die Ziele dargestellt.
- Was wird verfolgt bzw. soll erreicht werden?

Aktivität:

- Nach der Formulierung der Ziele, werden in diesem Bereich die Aktivitäten zur Erreichung der Ziele aufgeführt.

Erläuterung der Aktivitäten:

- Sind die Aktivitäten nicht eindeutig, folgen in diesem Abschnitt Erklärungen und Hilfestellungen. Diese sind jedoch nur als Hilfestellungen zu betrachten.
- Oftmals wird in den Erläuterungen auf ein externes Dokument verwiesen, da die genaue Umsetzung in diesem Leitfaden zu umfangreich wäre.
- Teilweise werden hier auch Ergebnisse der TÜV Cybersecurity Studie 2023 [1], die kürzlich erschienen ist, zur Verdeutlichung des Stellenwertes angegeben.

Abbildung 10: Aufbau der Schritte des Leitfadens

- Verantwortlichkeiten:
  Im ersten Bereich werden die Verantwortlichkeiten dieses Schrittes ausgewiesen. Wer ist insbesondere für die Bearbeitung, die Umsetzung bzw. die Inkraftsetzung zuständig?
- Ziele:
  Bei den Zielen wird beschrieben, welches Ziel dieser Schritt verfolgt bzw. was das Ziel der nachfolgenden Aktivitäten ist, um eine Art Selbstkontrolle durch den Nutzenden zu ermöglichen. Dadurch wird der/die Nutzende durch den Leitfaden geführt und das Verständnis für den jeweiligen Punkt erhöht.
- Aktivität:

  Unter diesem Punkt sind die Aktivitäten bzw. Arbeitspakete für den jeweiligen Schritt aufgeführt und kurz beschrieben.

- Erläuterungen zur Aktivität:

  Dieser Punkt enthält ergänzende Erläuterungen, Hilfestellungen und Informationen für ein besseres Verständnis für die Durchführung der Arbeitspakete dieses Schrittes. Die Normen und Richtlinien sind hierzu teilweise sehr ausführlich. Daher werden diese nur zusammengefasst beschrieben, da der Leitfaden keine Schritt-für-Schritt-Handlungsanweisung darstellt. Auf die Normen und Richtlinien sowie weiterführende zumeist freie Literatur wird am Ende eines Schrittes verwiesen.

Im Schlusswort des Leitfadens wird auf die regelmäßige Anpassung und Veränderung des ISMS aufgrund von sich ändernden Regeln, Vorschriften und/oder Gesetzen hingewiesen. Dieser Hinweis ist ebenfalls in der grafischen Übersicht zu finden.

In den zugrundeliegenden Normen und Richtlinien wird nicht zwischen produzierenden und nicht-produzierenden Unternehmen unterschieden [26, 27]. Daher und aufgrund der branchenübergreifenden Konzipierung des Leitfadens werden sowohl produzierende als auch nicht-produzierende Unternehmen angesprochen. Allerdings gibt es bei produzierenden Unternehmen Besonderheiten in der Umsetzung der Maßnahmen für ein ISMS, welche jedoch nicht Bestandteil dieses Leitfadens sind. Weitere Informationen, die in der Normenfamilie der DIN EN ISO 62443 und der VdS Richtlinie 10020 enthalten sind, sind als Verweise im Leitfaden aufgeführt.

So ist beispielsweise eine automatische Updatefunktion von Produktionsmaschinen nicht immer umsetzbar. Ein Beispiel hierfür ist die Aktualisierung des Virenschutzes. Die Steuerung eines Glasschmelzofens kann beispielsweise nicht einfach angehalten werden, da je nach Updatelänge dieser erkalten oder anderweitig ausfallen könnte und in Folge dessen nicht erneut gestartet werden kann.

Ähnlich dazu entfallen bei kleinen und sehr kleinen Unternehmen bei der Erstellung eines ISMS einige Maßnahmen bzw. werden nur sehr komprimiert angewandt. Diese Besonderheiten sind bei der Erstellung des Leitfadens mithilfe von Fußnoten und Anmerkungen berücksichtigt worden.

Dieser Leitfaden wurde auf der Basis der Normen DIN EN ISO/IEC 27000, 27001 und 27002 und der Richtlinien VdS 10000 und VdS 10005 erstellt. Da solche Normen und Richtlinien generell in einer technisch einwandfreien und rechtssicheren Sprache verfasst werden, sind sie häufig nur für Experten und Expertinnen unmittelbar nachvollziehbar. Daher ist es sinnvoll, für die IT-Verantwortlichen oder Informationssicherheitsbeauftragten von speziell kleinen und sehr kleinen Unternehmen, die nicht in der IT-Branche tätig sind, diese Formulierungen zu überarbeiten und ggf. mit Praxisbezügen zu ergänzen.

7 Schlusswort und Ausblick

Die vorliegende Arbeit zur Entwicklung eines in sich schlüssigen Leitfadens zur Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen wurde im Rahmen des Projekts „Netzwerk Mittelstand-Digital“ an der Hochschule Hannover in Form einer Bachelorarbeit verfasst.

Durch verschiedene Institutionen, Behörden und Verbände ist das Angebot an Normen, Richtlinien, technischen Standards, anderen Vorschriften und Informationen zum Thema Informationssicherheit sehr groß und für die Endanwendenden oftmals unübersichtlich.

Auf der Grundlage der DIN EN ISO/IEC 27000, 27001 und 27002 sowie der VdS-Richtlinien VdS 10000 und 10005 und den Werkzeugen, die das Bundesministerium für Sicherheit in der Informationstechnik zur Verfügung stellt, wurde dieser Leitfaden insbesondere für die Anwendung in sehr kleinen, kleinen und mittleren Unternehmen entwickelt.

Dazu wurden die betrachteten Normen, Richtlinien und Veröffentlichungen gesichtet, ausgewertet und in Handlungsschritten zusammengefasst. Weiterhin wurden diese mit Erläuterungen versehen, um die Handlungsschritte für Nicht-Experten in der Umsetzung so verständlich und nachvollziehbar wie möglich zu gestalten.

Auf diese Art und Weise ist ein branchenneutraler Leitfaden für KMU entstanden.

Der Leitfaden stellt ein in sich geschlossenes Dokument dar, welches losgelöst von dieser Arbeit verwendet werden kann. Er enthält eine Art vollständiger Checkliste, womit er die Umsetzung eines ISMS unterstützt. Detaillierte Beschreibungen der Umsetzung sind allerdings nicht im Leitfaden enthalten, weil diese den Umfang des Leitfadens um ein Vielfaches erhöhen würden und der Zweck eines Leitfadens damit verfehlt würde.

Daher sind zur Unterstützung bei der Umsetzung der Schritte des Leitfadens die Detailangaben aus den zugrunde liegenden Normen, Richtlinien und technischen Standards sowie die verwiesene Literatur heranzuziehen.

Der Leitfaden beruht auf den aktuellen Rahmenbedingungen im Bereich der Informationssicherheit, muss aber zukünftigen Änderungen in diesem Bereich angepasst werden, damit der Leitfaden weiter erfolgreich genutzt werden kann.

In einer Dokumentation [65] von „WissenHoch2“ wurde vor kurzem gezeigt, dass viele Geräte (insbesondere Geräte aus der Produktion) noch immer ungesichert mit dem Internet verbunden sind, was Kriminellen den Zugriff auf Informationen ohne größere Hindernisse deutlich erleichtert. Demnach benötigt der Angreifende ausschließlich einen Computer mit Internetzugang und etwa 20 Minuten, um eine ungesicherte Industriesteuerung (bspw. Industrieroboter, Krankenhaus, Kläranlage, Staudamm) ausfindig zu machen. Ist der Angreifende einmal unbemerkt im System, kann er/sie sich in aller Ruhe überlegen, welcher Schaden angerichtet werden kann.

In einer weiterführenden Arbeit könnte der Leitfaden für KMU dahingehend erweitert werden, dass dieser zusätzlich auf KMU mit produzierendem Gewerbe mit industriellen Automatisierungssystemen bezogen wird.

Dafür bietet sich u. a. die VdS 10020 an, die die Implementierung eines ISMS mithilfe von Interpretationen und Umsetzungsvorschlägen speziell für industrielle Automatisierungssysteme (produzierende Unternehmen) beschreibt.

Eine weitere Möglichkeit den Leitfaden für KMU zu erweitern, besteht darin, den Leitfaden um Anforderungen für KMU, die der kritischen Infrastruktur zugeschrieben werden, zu erweitern, da diese noch mehr durch Cyberangriffe gefährdet sind. Aufgrund des kritischen Status können diese Angriffe zu einem erheblichen Schaden für die Allgemeinheit und zu einer Gefahr für die öffentliche Sicherheit führen [9].

Bei der Erweiterung des Leitfadens um diese Unternehmen muss das Wording angepasst werden. Für diese Unternehmen sind die Anforderungen nicht nur halb-bindend, wie für alle anderen KMU, sondern verpflichtend, da das zweite IT-SiG [38] bzw. das BSI-Gesetz [36] eine Zertifizierung nach anerkanntem Standard vorschreibt.

Einige Beispiele werden im Folgenden aufgezählt:

- Beispielsweise sind KRITIS-Unternehmen dazu verpflichtet, IT-Sicherheitsvorfälle ab einer gewissen Größe zu melden.
- Weiterhin sind sie dazu verpflichtet ein ISMS nach geltendem Standard (oder ähnliches Sicherheitsmanagement) einzuführen.
- Jedes KRITIS-Unternehmen muss sich beim BSI registrieren und einen Ansprechpartner benennen.

8 Abbildungsverzeichnis

9 Literatur

[1] dpa-AFX. „Cyberangriffe werden häufiger - Gesetzliche Regelungen gefordert.” https://www.onvista.de/news/2023/06-12-roundup-cyberangriffe-werden-haeufiger-gesetzliche-regelungen-gefordert-10-26143126 (Zugriff am: 18. Juni 2023).

[2] Rechnungswesen-verstehen.de. „Asset.” https://www.rechnungswesen-verstehen.de/lexikon/asset.php (Zugriff am: 18. Juni 2023).

[3] Your Insider GmbH. „Grundlagen des Risikomanagements: Assets, Schwachstellen und Bedrohungen.” https://www.dsgvo-support.de/grundlagen-des-risikomanagements-assets-schwachstellen-und-bedrohungen/ (Zugriff am: 18. Juni 2023).

[4] DUDEN. „Cy-ber-at-ta-cke, die.” https://www.duden.de/rechtschreibung/Cyberattacke (Zugriff am: 19. Juni 2023).

[5] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-3 - Risikomanagement.” https://www.bsi.bund.de/dok/10027822 (Zugriff am: 18. Juni 2023).

[6] Europäische Kommission. „Gelten die Vorschriften für KMU?: Datenschutz-Grundverordnung bei KMU.” https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_de (Zugriff am: 19. Juli 2023).

[7] Avira. „Was ist der Unterschied zwischen Echtzeitschutz und System-Scanner?” https://support.avira.com/hc/de/articles/360000153538-Was-ist-der-Unterschied-zwischen-Echtzeitschutz-und-System-Scanner- (Zugriff am: 20. Juni 2023).

[8] Europäische Kommission, *Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen.* Zugriff am: 22. Februar 2023. [Online]. Verfügbar unter: http://data.europa.eu/eli/reco/2003/361/oj

[9] Bundesamt für Sicherheit in der Informationstechnik. „Was sind Kritische Infrastrukturen?: Definition KRITIS.” https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (Zugriff am: 19. Juni 2023).

[10] Dipl. Päd. Uta Reimann-Höhn. „Einen Leitfaden erstellen - Erklärung und Beispiele.” https://reimann-hoehn.de/der-leitfaden-erklaerung-und-beispiel/ (Zugriff am: 18. Juni 2023).

[11] Bundesamt für Sicherheit in der Informationstechnik. „Man-In-The-Middle-Angriff.” https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html

[12] Stephan Baumann. „Definition Normen - Standards: Normen.” https://www.ihk.de/koblenz/unternehmensservice/innovation-und-technologieberatung/normung-und-normen/definition-normen-standards-3325396 (Zugriff am: 19. Juni 2023).

[13] RWB Rechtswörterbuch. „Verfassungsrecht: Richtlinie.” https://www.rechtswoerterbuch.de/recht/r/richtlinien/ (Zugriff am: 19. Juni 2023).

[14] Prof. Dr.-Ing. Karl-Heinz Niemann, *IT-Sicherheit in Produktionsanlagen: Vorlesungsskript zur Vorlesung.* Zugriff am: 18. Juni 2023.

[15] BWLWissen.net. „Stakeholder." https://bwl-wissen.net/definition/stakeholder (Zugriff am: 19. Juni 2023).

[16] Baunetz_Wissen. „Glossar: VdS." https://www.baunetzwissen.de/glossar/v/vds-50339 (Zugriff am: 15. April 2023).

[17] Sacher. „SACHERTORTEN REZEPT: EIN REZEPT, DAS WIR TEILEN KÖNNEN." https://www.sacher.com/de/original-sacher-torte/rezept/ (Zugriff am: 19. Juni 2023).

[18] Bundeskriminalamt (BKA), *Bundes-lage-bild Cyber-crime 2021*, 2022. Zugriff am: 18. Juni 2023. [Online]. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110

[19] Bundesamt für Sicherheit in der Informationstechnik. „Die Lage der IT-Sicherheit in Deutschland." https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (Zugriff am: 18. Juni 2023).

[20] VdS Schadenverhütung GmbH. „Mindestanforderungen an die Informationssicherheit für Klein- und Kleinstunternehmen und Handwerksbetriebe." https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10005-mindestanforderungen-an-die-it-sicherheit-fuer-klein-und-kleinstunternehmen (Zugriff am: 18. Juni 2023).

[21] Maurice Shahd. „TÜV Cybersecuritystudie 2023." https://www.tuev-verband.de/studien/cybersicherheit-in-deutschen-unternehmen (Zugriff am: 18. Juni 2023).

[22] ZDNet-Redaktion. „Jedes 10. Unternehmen Opfer eines Hackerangriffs: Cybersecurity-Studie TÜV-Verband: Phishing und Erpressungssoftware häufigste Angriffsmethoden / Cyber Resilience Act zügig verabschieden." https://www.zdnet.de/88409783/1-von-10-unternehmen-im-jahr-2022-opfer-eines-hackerangriffs/ (Zugriff am: 18. Juni 2023).

[23] *DIN EN ISO/IEC 27000:2020-06, Informationstechnik_- Sicherheitsverfahren_- Informationssicherheitsmanagementsysteme_- Überblick und Terminologie (ISO/IEC_27000:2018); Deutsche Fassung EN_ISO/IEC_27000:2020,* DIN, Berlin.

[24] *DIN EN ISO/IEC 27001:2017-06, Informationstechnik_- Sicherheitsverfahren_- Informationssicherheitsmanagementsysteme_- Anforderungen (ISO/IEC_27001:2013 einschließlich Cor_1:2014 und Cor_2:2015); Deutsche Fassung EN_ISO/IEC_27001:2017,* DIN, Berlin.

[25] *DIN EN ISO/IEC 27002:2017-06, Informationstechnik_- Sicherheitsverfahren_- Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC_27002:2013 einschließlich Cor_1:2014 und Cor_2:2015); Deutsche Fassung EN_ISO/IEC_27002:2017,* DIN, Berlin.

[26] *VdS 10000 - Informationssicherheits-Managementsystem für kleine und mittlere Unternehmen (KMU),* VdS Schadenverhütung GmbH.

[27] *VdS 10005 - Mindestanforderungen an die IT-Sicherheit für Klein- und Kleinstunternehmen,* VdS Schadenverhütung GmbH.

[28] Andreas Bachmann. „Geschichte der ISO 27001." https://blog.adacor.com/geschichte-iso-27001_1725.html (Zugriff am: 18. Juni 2023).

[29] G. Disterer, „ISO/IEC 27000, 27001 and 27002 for Information Security Management," *JIS*, Jg. 04, Nr. 02, S. 92–100, 2013, doi: 10.4236/jis.2013.42011.

[30] M. Brenner, N. gentschen Felde, W. Hommel, S. Metzger, H. Reiser und T. Schaaf, *Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung,* 4. Aufl. München: Hanser, 2022. Zugriff am: 18. Juni 2023.

[31] Stefan Stroessenreuther. „ISO 27002 – Leitfaden für die Umsetzung der Informationssicherheit: ISO 27002 – Leitfaden." https://smct-management.de/iso-27002-leitfaden-fuer-die-umsetzung-der-informationssicherheit/ (Zugriff am: 18. Juni 2023).

[32] Dr Edward Humphreys, Pierre Sasseville. „SC27 STANDING DOCUMENT SD11: 2022 (2)." https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/sc27-sd11-sc-27-structure-members-and-work-programme-data.pdf (Zugriff am: 18. Juni 2023).

[33] *DIN EN ISO/IEC 27001:2023-04, Informationssicherheit, Cybersicherheit und Datenschutz_- Informationssicherheitsmanagementsysteme_- Anforderungen (ISO/IEC_27001:2022); Deutsche und Englische Fassung prEN_ISO/IEC_27001:2023,* DIN, Berlin. [Online]. Verfügbar unter: https://www.beuth.de/de/norm-entwurf/din-en-iso-iec-27001/365634117

[34] VdS Schadenverhütung GmbH. „Informationssicherheits-Management mit Zertifikat." https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu (Zugriff am: 18. Juni 2023).

[35] Bundesamt für Sicherheit in der Informationstechnik. „Arbeitsbeispiel RECPLAST GmbH." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/Recplast.html (Zugriff am: 18. Juni 2023).

[36] Bundesministerium der Justiz, *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik: BSI-Gesetz - BSIG*, 2009. Zugriff am: 18. Juni 2023. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[37] Bundesministerium der Justiz, *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme: IT-Sicherheitsgesetz*, 2015. Zugriff am: 18. Juni 2023. [Online]. Verfügbar unter: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf

[38] Bundesministerium der Justiz, *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme: IT-Sicherheitsgesetz 2.0*, 2021. Zugriff am: 18. Juni 2023. [Online]. Verfügbar unter: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf

[39] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-2 - IT-Grundschutz-Methodik." https://www.bsi.bund.de/dok/10027846 (Zugriff am: 18. Juni 2023).

[40] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-4 - Business Continuity Management: Community Draft." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (Zugriff am: 18. Juni 2023).

[41] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 100-4 - Notfallmanagement." https://www.bsi.bund.de/dok/6782544 (Zugriff am: 18. Juni 2023).

[42] Bundesamt für Sicherheit in der Informationstechnik. „IT-Grundschutz-Kompendium: Werkzeug für Informationssicherheit." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (Zugriff am: 18. Juni 2023).

[43] *DIN SPEC 27076:2023-05, IT-Sicherheitsberatung für Klein- und Kleinstunternehmen,* DIN, Berlin.

[44] Stefanie Siriu. „Schutzziele der Informationssicherheit." https://www.haufe.de/compliance/management-praxis/informationssicherheit/schutzziele-der-informationssicherheit_230130_483172.html (Zugriff am: 18. Juni 2023).

[45] Unbekannter Autor, *Keine Kette ist stärker als ihr schwächstes Glied.* Zugriff am: 18. Juni 2023.

[46] ISACA Germany Chapter e.V. „Implementierungsleitfaden ISO/IEC 27001:2013: Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013." https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf (Zugriff am: 18. Juni 2023).

[47] Der ProzessManager. „Was ist ein PDCA-Zyklus? Plan-Do-Check-Act einfach erklärt." https://der-prozessmanager.de/aktuell/wissensdatenbank/pdca-zyklus (Zugriff am: 18. Juni 2023).

[48] J. Naumann, *ISO/IEC 27001 ISO/IEC 27002 und IT-Grundschutz: Schnelleinstieg Informationssicherheit 2022,* 3. Aufl. Norderstedt: BoD – Books on Demand, 2023. Zugriff am: 18. Juni 2023.

[49] Marian Thöne, *Organigramm eines Informationssicherheitsteams: - Eigene Entwicklung eines Schaubildes*, 2023.

[50] Europäische Union, *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR): Datenschutz-Grundverordnung (DSGVO).* Zugriff am: 18. Juni 2023. [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679

[51] Bundesministerium der Justiz, *Bundesdatenschutzgesetz - § 38 Datenschutzbeauftragte nichtöffentlicher Stellen: BDSG.* Zugriff am: 18. Juni 2023. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/bdsg_2018/__38.html

[52] FRANK WIERCKS. „DS-GVO bleibt für KMU eine große Herausforderung." https://www.trialog-magazin.de/wirtschaft-und-recht/datenschutz-verbraucher/ds-gvo-ist-fuer-kmu-ein-grosses-problem/#:~:text=KMU%20m%C3%BCssen%20nur%20dann%20einen,insbesondere%2C%20da%20sie%20in%20gro%C3%9Fem (Zugriff am: 18. Juni 2023).

[53] Mark Semmler GmbH, Hg. *Das Portal rund um die VdS 10000: 10.3 Basisschutz.* Zugriff am: 5. Mai 2022. [Online]. Verfügbar unter: https://www.vds10000-portal.de/doku.php?id=10k_kommentiert_public:10:10.3

[54] *VdS 2007 : 2016-03 - Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen,* VdS Schadenverhütung GmbH.

[55] Lisa Ohl. „Was ist ein Leitfaden? Einfach erklärt." https://praxistipps.focus.de/was-ist-ein-leitfaden-einfach-erklaert_147300 (Zugriff am: 18. Juni 2023).

[56] Land Niedersachsen, vertreten durch die Niedersächsische Staatskanzlei. „Informationen zum Corona-Virus in Leichter Sprache." https://www.niedersachsen.de/Coronavirus/die-krankheit-corona-virus-185485.html (Zugriff am: 18. Juni 2023).

[57] „Grundgesetz für die Bundesrepublik Deutschland - Art. 10," in *Grundgesetz*, Artikel 10. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/gg/art_10.html

[58] „Grundgesetz für die Bundesrepublik Deutschland - Art. 73," in *Grundgesetz*, Artikel 73. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/gg/art_73.html

[59] tagesschau.de. „Nach Hackerangriff: Stadtverwaltung von Bad Langensalza wieder erreichbar." https://www.tagesschau.de/inland/regional/thueringen/mdr-hackerangriff-auf-stadtverwaltung-von-bad-langensalza-systeme-lahmgelegt-100.html (Zugriff am: 30. Juni 2023).

[60] d. op-online. „Cyberangriff auf Stadt Rodgau führt zu Ausfall der Servicesysteme." https://www.op-online.de/region/rodgau/cyberangriff-stadt-rodgau-ausfall-servicesysteme-stadtverwaltung-stadtwerke-hacker-angriff-it-92107552.html (Zugriff am: 30. Juni 2023).

[61] Continental. „Cyberangriff auf Continental." https://www.continental.com/de/presse/studien-publikationen/sonstige-publikationen/cyber-angriff-fragen-und-antworten/ (Zugriff am: 18. Juni 2023).

[62] enercity. „IT-Störung bei enercity." https://www.enercity.de/presse/betrieb-und-baustellen/2022/it-stoerung (Zugriff am: 18. Juni 2023).

[63] Üstra. „Nach Hackerangriff: Deutschlandticket im GVH für den 1. Juni buchbar, davor mit Übergangslösung, kein Einfluss auf 365-Job- und Sozialtickets." https://www.uestra.de/unternehmen/presse-medien/pressemitteilungen/details/2023/nach-

hackerangriff-deutschlandticket-im-gvh-fuer-den-1-juni-buchbar-davor-mit-uebergangs-loesung-kei/ (Zugriff am: 18. Juni 2023).

[64] Justin Arber. „Russische Hacker greifen Schweizer Technologieriesen ABB an: Erneut ist es Hackern gelungen, die Arbeit in einem Schweizer Unternehmen mittels Ransomware zu beeinträchtigen." https://www.20min.ch/story/hacker-greifen-schweizer-technologieriesen-abb-an-287737352826 (Zugriff am: 20. Juni 2023).

[65] WissenHoch2, *Cybercrime: Wie können wir uns schützen?* Zugriff am: 15. Juni 2023. [Online]. Verfügbar unter: https://www.3sat.de/wissen/wissenschaftsdoku/230615-sendung-cybercrime-wido-100.html

10 Anhang

Im Anhang sind die folgenden Dateien enthalten:

Anhangsbuchstabe	Anhangstitel
Anhang A	Leitfaden zur Einführung eines ISMS bei KMU
Anhang B	Aufgabenstellung der Bachelorarbeit

A. Leitfaden zur Einführung eines ISMS bei KMU

Hochschule Hannover

University of Applied Sciences and Arts

Fakultät I – Elektro und Informationstechnik

Fachgebiet: Automatisierungstechnik und Prozessinformatik

– Leitfaden –

„Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen“

Autor: Marian Thöne

Erarbeitet im Rahmen einer Bachelorarbeit.

Erstprüfer: Prof. Dr.-Ing. Karl-Heinz Niemann

Zweitprüfer: M. Eng. Jan-Niklas Puls

I Versionshistorie

Version	Datum	Bemerkung	Erstellende Person
1.0	02.07.2023	Erstausgabe	MarTh
1.1	31.07.2023	Korrigierte Erstausgabe – Kommentare von Erst- und Zweitprüfer – Hinzufügen der „CC BY 4.0“ Lizenz	MarTh
1.2	22.09.2023	Einarbeitung von weiteren Korrekturen	Jan-Niklas Puls
2.0	12.10.2023	Zweitausgabe (Veröffentlichung) – Einpflegen von Kommentaren – Hinzufügen des Haftungsausschlusses – Hinzufügen des Autors	MarTh

Der Leitfaden wurde als Teil einer Bachelorarbeit während der Kooperation der Hochschule Hannover mit dem Mittelstand-Digitalzentrum Hannover erarbeitet.

II Haftungsausschluss

Die diesem Dokument zu Grunde liegenden Informationen wurden mit größtmöglicher Sorgfalt recherchiert und zusammengestellt. Dennoch wird es ohne eine Gewährleistung zur Verfügung gestellt. Der Autor lehnt ausdrücklich jede Art von vertraglicher oder gesetzlicher Haftung für dieses Dokument ab. In keinem Fall ist der Autor für Schäden verantwortlich, die durch Fehler oder fehlende Informationen in diesem Dokument entstehen könnten. Logos und Markennamen werden ohne Hinweis auf ggf. bestehende Schutzrechte verwendet.

III Inhaltsverzeichnis

1 Warum dieser Leitfaden?

Die Sicherheit von Informationen gewinnt für Unternehmen in den letzten Jahren an immer größerer Bedeutung, nicht nur durch das stetig steigende, sondern auch durch die ökonomische Bedeutung von Sicherheitsvorfällen.

Das belegt auch eine kürzlich veröffentlichte Studie (TÜV Cybersecuritystudie 2023), die vom TÜV-Verband in Auftrag gegeben wurde [1–3].

- 98 % der befragten Unternehmen empfinden Cyberangriffe als ernste Gefahr.
- 76 % der befragten Unternehmen sehen Vorteile in einem hohen IT-Sicherheitsniveau.

Die Bedeutung der Informationssicherheit bei Unternehmen in Deutschland weist laut dieser Studie große Unterschiede je nach Größe des Unternehmens auf.

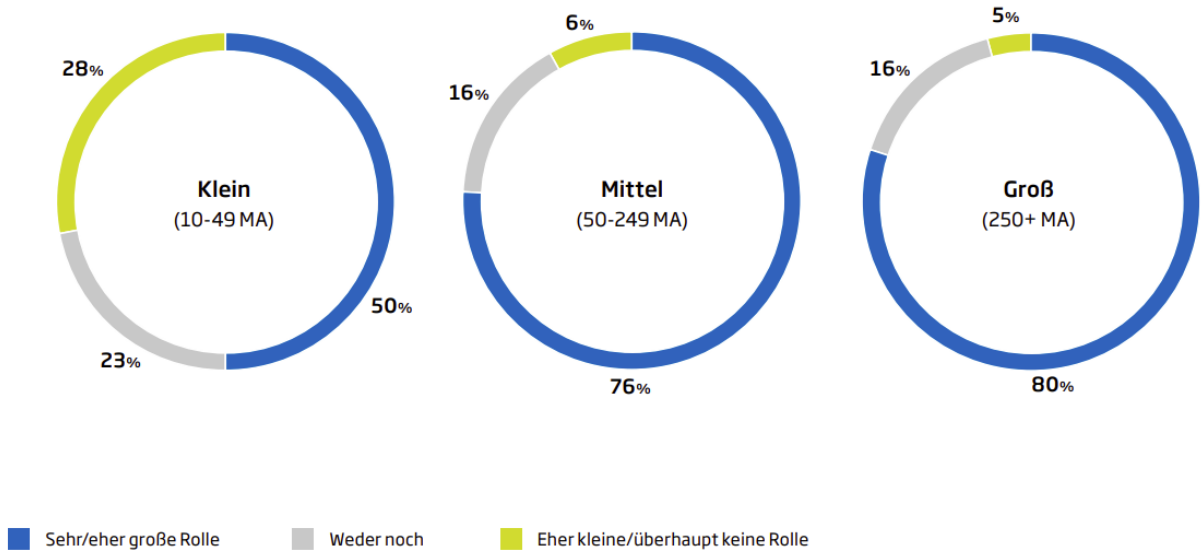

Abbildung 1: Bedeutung der Cybersecurity in Unternehmen [1, S. 8]

Abbildung 1 zeigt, dass bei größeren Unternehmen mit mehr als 250 Mitarbeitenden lediglich bei etwa 5 % der Unternehmen die Informationssicherheit nahezu keine Rolle spielt. Je kleiner die Unternehmen werden, desto größer wird der Anteil der Unternehmen, bei denen die Informationssicherheit keine größere Rolle spielt. In dieser Erhebung wurden lediglich Unternehmen mit mehr als zehn Mitarbeitenden befragt. Die Tendenz der Grafik lässt aber darauf schließen, dass die Rolle der Informationssicherheit bei Unternehmen mit weniger als zehn Mitarbeitenden noch geringer ausfallen wird, als bei kleinen und mittleren Unternehmen [3, S. 8].

Um diese Tendenz aufzuhalten, bietet ein Informationssicherheitsmanagementsystem (ISMS), basierend auf (inter-)nationalen Normen, eine Grundstruktur für den effizienten und effektiven Umgang mit einer ganzheitlichen Sicherheitsstrategie. [4, S. 5]

Eine solche ganzheitliche Sicherheitsstrategie ist sowohl für produzierende als auch nicht produzierende Unternehmen von Bedeutung.

In der Wissenschaftsdokumentation „Cybercrime – Wie können wir uns schützen?“ ergab ein Test, dass viele Steuerungen von Produktionsmaschinen noch immer frei über das Internet zugänglich sind und von Dritten kontrolliert werden können. Von der Manipulation des Lichtes bis zur Steuerung von kritischen Ventilen oder ganzen Maschinen gäbe es zahlreiche Angriffsmöglichkeiten. Dieses Beispiel zeige sehr deutlich den Handlungsbedarf bei produzierenden Unternehmen – insbesondere bei sehr kleinen, kleinen und mittleren Unternehmen [5].

Abhängig von der Branche und den zu schützenden Informationen variiert die Ausrichtung der Ziele des ISMS. Die Erreichung dieser Ziele insbesondere bei KMU erfordert aufgrund von fehlender Praxis und fehlenden Ressourcen ein gewisses Maß an Anpassung und näheren Erläuterungen.

Der vorliegende Leitfaden zur Einführung eines ISMS bei KMU basiert im Wesentlichen auf den VdS-Richtlinien VdS 10000 [6] und VdS 10005 [7]. Er enthält eine grundlegende Zusammenstellung der Forderungen aus den zurzeit relevanten (inter-) nationalen Vorschriften und Normen und richtet sich an die Unternehmen, die ein ISMS zur Sicherheit Ihres Unternehmens aufbauen oder optimieren wollen.

Für größere KMU sind auch die Normen der DIN EN ISO/IEC 27000-Normenfamilie relevant. Der Fokus liegt in diesem Leitfaden jedoch auf den kleineren KMU.

Bei kleinen Unternehmen ist der Anteil derer, die ihre Informationssicherheit nicht auf der Basis von Normen und Standards implementieren, mit 38 % sehr hoch – bei mittleren Unternehmen ist dieser mit 12 % deutlich geringer. Mithilfe dieses Leitfadens sollen auch kleine Unternehmen unterstützt werden, ihre Informationssicherheit durch Normen und Standards zu verbessern [3, S. 42].

Der Leitfaden ist ein eigenständiges und in sich abgeschlossenes Dokument. Es versetzt den Anwendenden in die Lage, mit einer Art Checkliste das ISMS ohne Vorkenntnisse zu etablieren. Durch die Beschreibung von Zielen und weitergehenden Erläuterungen werden die Anwendenden zielgerichtet zu einem ISMS geführt. Als „Schritt-für-Schritt-Bedienungsanleitung“ bzw. Schilderung der genauen Umsetzung ist dieser Leitfaden jedoch nicht anzusehen, da dies nicht das Ziel eines Leitfadens darstellt. Ein Leitfaden soll leiten, aber nicht die genaue Vorgehensweise vorgeben. Deswegen werden in vielen Fällen nur Beispiele und Hilfen angeführt und es wird auf die relevanten Normen und Richtlinien verwiesen, sodass das Grundkonzept umgesetzt werden kann.

Sofern weitere Informationen erforderlich sind, wird in jedem Schritt des Leitfadens auf die entsprechenden Normen verwiesen, sodass dort die weiterführenden Informationen entnommen werden können. Für Unternehmen bis 50 Mitarbeitende ist darüber hinaus ein Blick in die seit 2023 veröffentlichte und frei zur Verfügung stehende DIN SPEC 27076 empfehlenswert. Hier werden Problemstellungen und potentielle Lösungsmaßnahmen vorgestellt.

Allgemein wird zwischen produzierenden und nicht produzierenden Unternehmen unterschieden. Der Leitfaden gilt hierbei generell für alle Unternehmen. Bei produzierenden Unternehmen sind einige Maßnahmen jedoch nicht umsetzbar. Einige dieser Ausnahmen sind im Leitfaden angemerkt. Die Umsetzung dieser Maßnahmen ist jedoch nicht Bestandteil des Leitfadens. Für die besonderen Anforderungen von industriellen Automatisierungssystemen können interessierte Unternehmen die Maßnahmen und technischen Aspekte in der Norm DIN EN IEC 62443-2-1 [8] und der Richtlinie VdS 10020 nachlesen.

Zu Beginn wird in Kapitel 2 der Aufbau des Leitfadens mithilfe eines Schaubildes visualisiert. Im darauffolgenden Kapitel (Kapitel 3) werden dann die einzelnen Schritte des Schaubildes aus Kapitel 2 erklärt, bevor diese in Kapitel 4 detailliert beschrieben werden. Kapitel 5 schließt den Leitfaden ab.

*Laut der TÜV Cybersecurity Studie 2023 sagen **lediglich etwa 18 %** der Befragten, dass die Informationssicherheit die **Produktivität des Unternehmens verringere** bzw. neue **Innovationen hemmt*** [3, S. 23].

An diesem Zitat wird deutlich, dass die Mehrheit der Befragten keine oder nur sehr geringe Beeinträchtigungen durch die Implementierung eines ISMS erwartet.

2 Leitfaden zur Einführung eines ISMS bei KMU – Aufbau

Das nachfolgende Schaubild zeigt den Aufbau des Leitfadens. Diese Farben finden sich ebenfalls in den Rahmen der einzelnen Schritte der detaillierten Beschreibungen in Kapitel 4 wieder.

3 Leitfaden zur Einführung eines ISMS bei KMU – Erläuterungen

Dieses Kapitel dient als Information, um den Aufbau des nächsten Kapitels zu erklären und den Umgang damit zu erleichtern.

Jeder Schritt im nächsten Kapitel besteht immer aus den folgenden Bereichen:

Schritt: Titel

Verantwortlichkeiten:

- Hier werden die Verantwortlichkeiten des Vorgangs definiert und ggf. Aufgaben dieser in Bezug auf den Vorgang beschrieben.

Ziele:

- Hier werden die Ziele dargestellt.
- Was wird verfolgt bzw. soll erreicht werden?

Aktivität:

- Nach der Formulierung der Ziele, werden in diesem Bereich die Aktivitäten zur Erreichung der Ziele aufgeführt.

Erläuterung der Aktivitäten:

- Sind die Aktivitäten nicht eindeutig, folgen in diesem Abschnitt Erklärungen und Hilfestellungen. Diese sind jedoch nur als Hilfestellungen zu betrachten.
- Oftmals wird in den Erläuterungen auf ein externes Dokument verwiesen, da die genaue Umsetzung in diesem Leitfaden zu umfangreich wäre.
- Teilweise werden hier auch Ergebnisse der TÜV Cybersecurity Studie 2023 [3] zur Verdeutlichung des Stellenwertes angegeben.

Manche Schritte und Informationssicherheitsrichtlinien sind in den VdS-Richtlinien für sehr kleine und/oder kleine Unternehmen nicht vorgesehen. Die Kennzeichnung dazu erfolgt mittels Fußnoten.

Wie im vorherigen Kapitel schon erwähnt, deutet die Farbe des Rahmens auf den jeweiligen Schritt im Schaubild des Leitfadens hin.

4 Leitfaden zur Einführung eines ISMS bei KMU – Schritte

Schritt 1: Analyse des Unternehmens

Verantwortlichkeiten:

- Die Geschäftsleitung gibt die Analyse des Ist-Zustandes des Unternehmens in Auftrag oder führt diese selber aus und ist für das Ergebnis verantwortlich.

Ziele:

- Übersicht aller vertraglichen Anforderungen und gesetzlichen Vorschriften
- Übersicht aller Stakeholder und Stakeholderinnen
- Scope-Dokument (Dokument über den Geltungsbereich)
- Erklärung zur Anwendbarkeit (SoA)

Aktivität:

- Analyse der Verträge des Unternehmens hinsichtlich der Anforderungen in Bezug auf die Informationssicherheit.
- Analyse der gesetzlichen Vorschriften, die das Unternehmen und Ihre Branche betreffen, in Bezug auf die Informationssicherheit.
- Ausführliche Bestimmung der **Stakeholder und Stakeholderinnen** und die Bedeutung jedes/jeder Einzelnen.
- Bestimmung des **Geltungsbereich** des ISMS und Durchführung einer Umfeldanalyse (relevante organisatorische und technische Schnittstellen).
- Analyse der Anwendbarkeit der Maßnahmen zur Informationssicherheit in dem Unternehmen und Dokumentation des Ergebnisses in der sogenannten „**Erklärung zur Anwendbarkeit**“ (SoA – engl. **S**tatement **o**f **A**pplicability).

Erläuterung der Aktivitäten:

- Analyse der Verträge des Unternehmens hinsichtlich der Anforderungen in Bezug auf die Informationssicherheit.
  - Welche Daten gibt es im Unternehmen und wo werden diese gelagert?
  - Welche Hard-/Software wird verwendet?
  - Wer ist im Unternehmen für die Informationssicherheit zuständig?
  - Wer trägt die Gesamtverantwortung für die Informationssicherheit im Unternehmen?
  - Weitere beispielhafte Fragen können in dem kostenfrei zur Verfügung stehenden Dokument „**DIN SPEC 27076**“ [8] nachgelesen werden.
- Analyse der gesetzlichen Vorschriften, die das Unternehmen und die Branche betreffen, in Bezug auf die Informationssicherheit.
  - IT-SiG 2.0 – IT-Sicherheitsgesetz 2.0
  - NIS-Richtlinie – Richtlinie für die Gewährleistung einer hohen Netzwerk- und Informationssicherheit (nur für KRITIS relevant)
  - NIS-2-Richtlinie – Nachfolger der NIS-Richtlinie

    (wird aktuell in nationales Recht überführt)
  - TTDSG – Telekommunikation-Telemedien-Datenschutz-Gesetz
  - DSGVO – Datenschutzgrundverordnung
  - Aktien- und GmbH-Recht – Vorgaben zum Risikomanagement
  - KRITIS 2.0 – Verordnung zur Bestimmung von kritischen Infrastrukturen
    Info: Dieser Leitfaden bezieht sich **nicht** auf KRITIS-Unternehmen. Der Vollständigkeit halber ist die Verordnung hier trotzdem aufgeführt
  - EU Cyber Resilience Act [9]
  - weitere Gesetze und Vorschriften z. B. von der Handwerkskammer
- Ausführliche Bestimmung der **Stakeholder und Stakeholderinnen** und die Bedeutung jedes/jeder Einzelnen.
  - Kunden/Kundinnen, Lieferanten/Lieferantinnen, Dienstleistende, Gesetzgeber/Gesetzgeberinnen, Gläubiger/Gläubigerinnen, Gesellschaft
  - Mitarbeitende, Manager/Managerinnen, Eigentümer/Eigentümerinnen

- Bestimmung des **Geltungsbereichs** des ISMS und Durchführung einer Umfeldanalyse (relevante organisatorische und technische Schnittstellen).

  Info: Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in der VdS Richtlinie VdS 10005 nicht vorgeschrieben.

  - Erstellung eines Netzstrukturplan aller maßgeblichen Systeme und Komponenten
  - Das BSI bietet hierzu eine Informationsseite auf seiner Homepage an, auf welcher die Wahl des Geltungsbereiches beschrieben wird [10].
  - ISO 31000:2018 – 6.3.2 und 6.3.3 stellen Leitfäden für die Vollständigkeit der Dokumentation zur Verfügung [11]

  Analyse der Anwendbarkeit der Maßnahmen zur Informationssicherheit in dem Unternehmen und Dokumentation des Ergebnisses in der

  „**Erklärung zur Anwendbarkeit**“ (SoA).

  Info: Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in der VdS-Richtlinie VdS 10005 nicht vorgeschrieben.

  In einer solchen Erklärung zur Anwendbarkeit steht die Anwendbarkeit der Maßnahmen aus dem Anhang A der ISO 27001 [12]. Diese Erklärung kann mittels einer Tabelle durchgeführt und dokumentiert werden.
  Eine mögliche Tabellenstruktur wird nachfolgend dargestellt.

Tabelle 1: Beispielhafte Tabellenstruktur zur Umsetzung einer SoA

Maßnahmen	Anforderungen			Umsetzung	Status
	Vertraglich	Gesetzlich	Regulatorisch		
Überprüfung der Informationssicherheitsrichtlinien					
Informationssicherheitsrollen und -verantwortlichkeiten					
Sicherheitsüberprüfung					
…					

Diese Tabelle stellt lediglich eine beispielhafte Struktur dar und ist individuell auf die jeweiligen Bedürfnisse anzupassen. Zudem sollte diese Tabelle um die im Anhang A der DIN EN ISO/IEC 27001 [12] stehenden Anforderungen ergänzt werden.
Für eine Zertifizierung ist es Pflicht, diese Anforderungen zu berücksichtigen.

Schritt 2: Informationssicherheitsleitlinie [1]

Verantwortlichkeiten:

- Die Geschäftsleitung ist für die Inkraftsetzung einer Informationssicherheitsleitlinie verantwortlich und muss dafür sorgen, dass diese jährlich geprüft und ggf. aktualisiert wird.

Ziele:

- Mit dieser Leitlinie soll der Stellenwert der Informationssicherheit im Unternehmen festgelegt werden.

Aktivität:

- Erstellung einer Informationssicherheitsleitlinie.

Erläuterung der Aktivitäten:

Erstellung einer Informationssicherheitsleitlinie.

- Festlegung der Ziele und des Stellenwertes der Informationssicherheit im Unternehmen
- Definition aller erforderlichen Positionen und deren Aufgaben im Unternehmen
  - Geschäftsleitung
  - Informationssicherheitsbeauftragter/Informationssicherheitsbeauftragte
  - Informationsverantwortlicher/Informationsverantwortliche
  - Systemadministrator/Systemadministratorin
  - Projektverantwortliche
  - Externe (Lieferanten/Lieferantinnen)
  - Datenschutzbeauftragte(r)
  - Betriebsrat (Mitarbeitende)
  - Vorgesetzte
- Angaben von Konsequenzen bei Nichtbeachtung der Leitlinie.
- Das BSI hat für ein fiktives Unternehmen eine komplette Analyse durchgeführt und u. a. auch eine Sicherheitsleitlinie erstellt. Diese kann im Verweis [13] im Literaturverzeichnis nachgelesen werden und als Arbeitsgrundlage dienen.

[1] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Schritt 3: Risikoanalyse [2]

Verantwortlichkeiten:

- Die Geschäftsleitung ist für die verantwortungsbewusste Durchführung verantwortlich.

Ziele:

- Ausführliche Risikoanalyse der Informationssicherheit des Unternehmens

Aktivität:

- Durchführung einer ausführlichen Risikoanalyse.

Erläuterung der Aktivitäten:

- Eine Risikoanalyse besteht aus der **Identifikation**, der **Analyse** und der **Bewertung** von Risiken und definiert den IST-Zustand des Unternehmens.
- Nach dem BSI 200-3 Standard [14] sind folgende vier Schritte A – D für eine Risikoanalyse vorgesehen:

  A) Erstellung einer Gefährdungsübersicht (elementare und spezifische Gefährdungen) – (Kapitel 4 des BSI 200-3)

  - elementare Gefährdung: Feuer, Wasser, Naturkatastrophen, Stromausfall
    Info: Bei produzierendem Gewerbe ist dies ein wichtiger Punkt in der Risikoanalyse, da beispielsweise durch Stromausfälle oder Überflutungen (Wasser, Naturkatastrophen) die Produktion akut gefährdet sein kann.
  - spezifische Gefährdungen: auf das Unternehmen und den Standort bezogene spezifische Gefährdungen, die einen nennenswerten Schaden hervorrufen können

  B) Einstufung der Gefährdungen (Einschätzen und Bewerten) – (Kapitel 5 des BSI 200-3)

  - Einordnung der ermittelten Gefährdungen in vier Kategorien der **Eintrittshäufigkeit** (selten, mittel, häufig, sehr häufig)
  - Einordnung der ermittelten Gefährdungen in vier Kategorien der **Schadenshöhe** (vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend)

[2] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

- Bestimmung von vier Risikokategorien und Beschreibung dieser, um die Gefährdungen individuell einstufen zu können (im Anschluss an diese Erklärung ist eine Beispielmatrix für die Risikoanalyse mit beispielhaften Definitionen der Risikokategorien dargestellt.)

C) Behandlung der Risiken (Vermeidung, Reduktion, Transfer und Akzeptanz) – (Kapitel 6 des BSI 200-3)

- Bestimmung von für das Unternehmen geeigneten Risikobehandlungsoptionen
- Vermeidung: Ist das Risiko durch eine Umstrukturierung eines Geschäftsprozesses vermeidbar?
- Reduktion: Sind weitere Maßnahmen zur Reduktion möglich und sinnvoll?
- Transfer: Kann das Risiko an einen externen Dienstleistenden ausgelagert werden? (Outsourcing oder Versicherungen)
- Akzeptanz: Ist es möglich, die potentiellen Konsequenzen des Risikos zu akzeptieren?

D) Konsolidierung des Sicherheitskonzepts (Integration in das Sicherheitskonzept) – (Kapitel 7 des BSI 200-3)

Zusätzliche Maßnahmen müssen anhand folgender Kriterien überprüft werden:

- Ist diese Maßnahme für den vorgesehenen Zweck geeignet und widerspricht nicht den Sicherheitszielen oder anderen Maßnahmen des Unternehmens?
- Ist die Maßnahme transparent und klar beschrieben, sodass der Inhalt für Mitarbeitende ersichtlich und verständlich ist?
- Ist die Maßnahme angemessen in Bezug auf die Gefährdung?
- Stehen Kosten, Aufwand und Nutzen im Gleichgewicht?

Für die Risikoanalyse kann der ausführliche Leitfaden im BSI-Standard 200-3 des Bundesamtes für Sicherheit in der Informationstechnik [14] sowie die vom BSI beispielhafte Ausführung einer Risikoanalyse anhand des fiktiven Unternehmens Recplast [13] genutzt werden.

Produzierende Unternehmen können unter Zuhilfenahme der DIN EN IEC 62443-3-2 [15] Maßnahmen zur Risikoreduzierung identifizieren und festlegen, die speziell für industrielle Automatisierungssysteme oder Produktionsanlagen relevant sind. Mithilfe dieser Norm werden entsprechende Security-Gegenmaßnahmen durch sog. Security-Levels in den einzelnen Produktionsbereichen (Zonen) festgelegt.

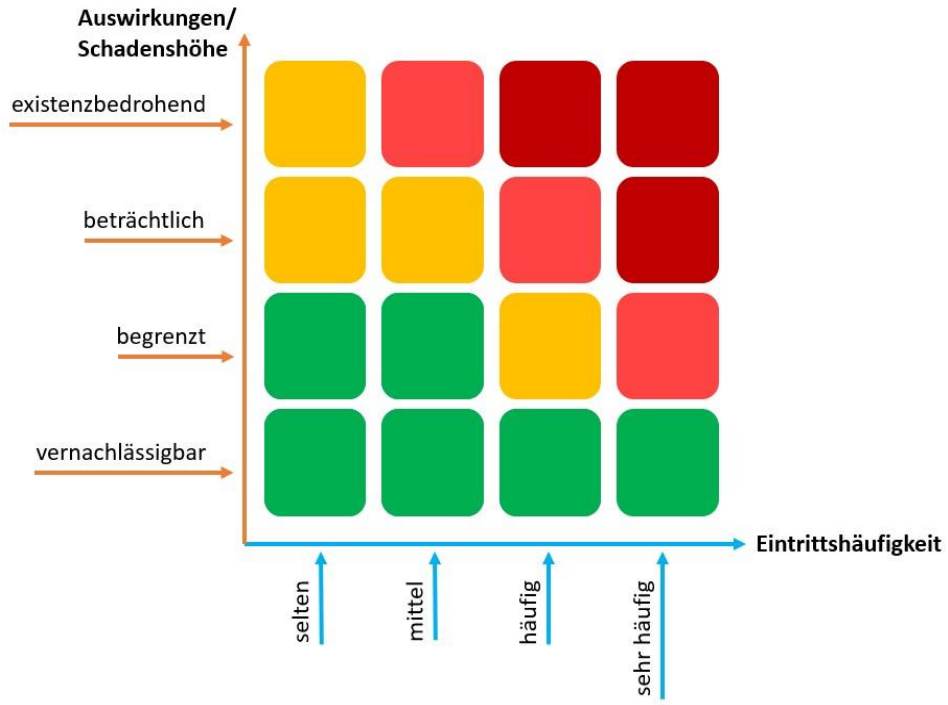

Abbildung 2: Beispiel einer Risikomatrix [6, S. 27]

Legende der Risikokategorien
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **einen** ausreichenden Schutz. **=> Aktuell keine Handlung oder Maßnahme notwendig**
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **möglicherweise keinen** ausreichenden Schutz. **=> Beobachten und stetige Überprüfung der Maßnahmen**
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **definitiv keinen** ausreichenden Schutz. **=> Handlungsbedarf, Neubewertung und regelmäßigere Überprüfung der Maßnahmen**
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **definitiv keinen** ausreichenden Schutz. **=> Dringender Handlungsbedarf! Sofortige Neubewertung bestehender Schutzmaßnahmen/Umsetzung neuer Maßnahmen**

Abbildung 3: Legende zur Grafik aus Abbildung 2 [vgl. 6, S. 28]

Schritt 4: Organisation der IT-Sicherheit

Verantwortlichkeiten:

- Die Geschäftsleitung ist für alle Entscheidungen verantwortlich, sollte jedoch die Verantwortung an einzelne Personen delegieren.

Ziele:

- Aufbau einer IT-Organisation

Aktivität:

- Benennung des/der Verantwortliche(n) in der Geschäftsleitung und Dokumentation dieser.
- Zuweisen von
  - mindestens einer Person für die **IT-Verantwortung**.
  - mindestens einer Person als **Vertretung der Belegschaft** (ggf. aus dem **Betriebsrat**). [3]
  - mindestens einer Person für die **Administration der Systeme**. [4]
  - mindestens einer Person für den **Datenschutz** (**Datenschutzbeauftragte**). [3, 5]
  - einer Person für die Aufgaben der/s **Informationssicherheitsbeauftragen (ISB)** zu. [3]

[3] Bei kleinen und sehr kleinen Unternehmen, entfallen diese Positionen. Bei sehr kleinen Unternehmen ernennt die Geschäftsleitung **eine(n)** Mitarbeitende(n) zum/zur Informationssicherheitsverantwortlichen. Diese(r) ist für die gesamte Umsetzung der Maßnahmen verantwortlich.

[4] Bei sehr kleinen Unternehmen (< 10 Mitarbeitende) wird trotz der beschränkten Verfügbarkeit von Mitarbeitenden **empfohlen**, dass die Geschäftsleitung einen/eine Mitarbeitende(n) zum/zur **Systemadministrator**(in) ernennt, die geforderten technischen Maßnahmen für die Informationssicherheit zu implementieren und zu administrieren.

[5] Ein(e) Datenschutzbeauftragte(r) ist nur erforderlich, wenn im Unternehmen **dauerhaft** Mitarbeitende mit der Handhabung von personenbezogenen Daten beschäftigt sind [16].

Erläuterung der Aktivitäten:

Die Vertretungen der einzelnen genannten Bereiche bilden das **Informationssicherheits-team** (kurz IST). Die Aufgabe des IST besteht in der Unterstützung des/der ISB bei folgenden Tätigkeiten:

- Erkennen und Bewerten neuer Bedrohungen und Schwachstellen
- Entwickeln und Bewerten von Maßnahmen zur Informationssicherheit
- Steuern und Koordinieren der Maßnahmen zur Informationssicherheit (unternehmensweit)

Doppelbelegungen einer Funktion sollten möglichst vermieden werden. Sind Doppelbelegungen nicht zu vermeiden oder im Unternehmen sinnvoll, sollte die Begründung dokumentiert und zu den Akten genommen werden.

Dokumentation dieses Schrittes.

Das nachfolgende Organigramm zeigt den Aufbau der Informationssicherheit nach der Richtlinie VdS 10000 [6].

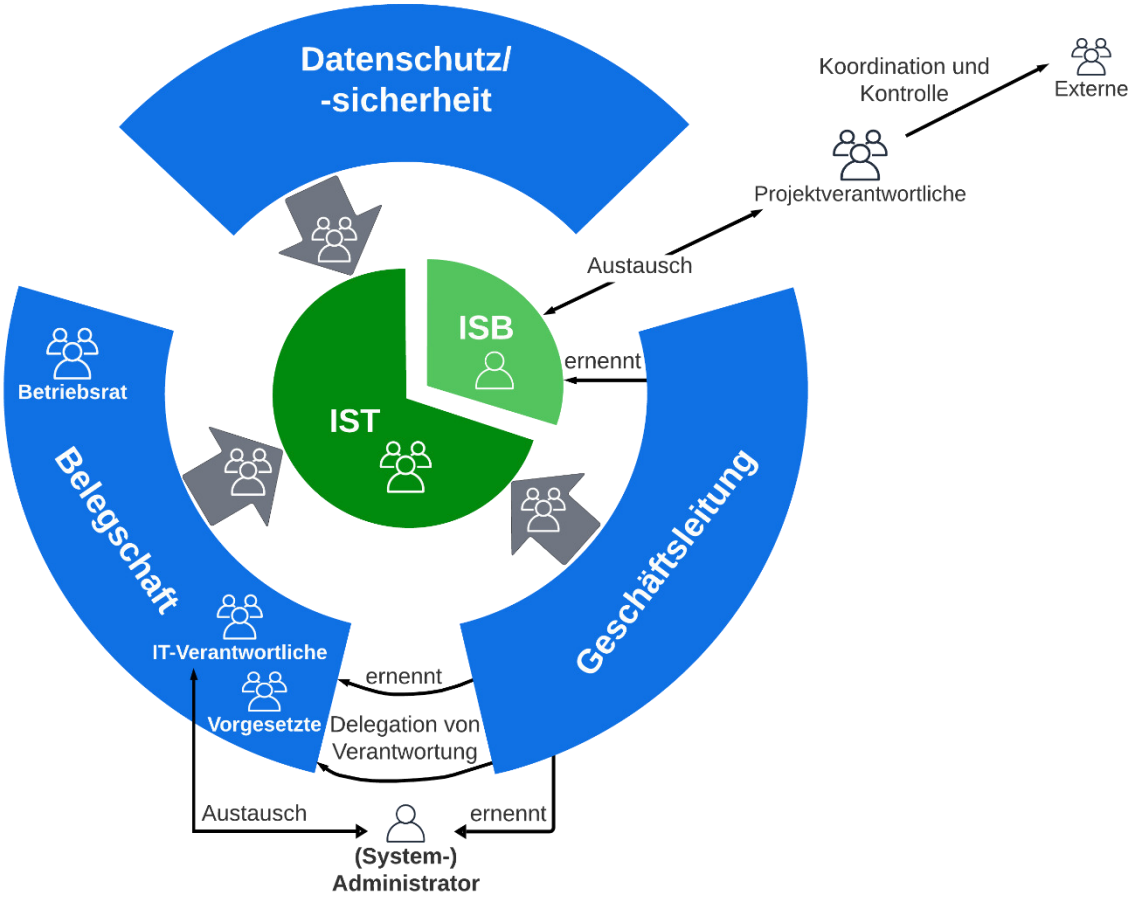

Abbildung 4: Organigramm der Informationssicherheit [17]

Schritt 5: Informationssicherheitsrichtlinien (ISR)

Eine Informationssicherheits**richt**linie ist ein unterstützendes Dokument der Informationssicherheits**leit**linie. In ihr werden weitergehende Regelungen für die Informationssicherheit getroffen und Maßnahmen dafür eingeführt.

Jede Richtlinie wird vom IST in Zusammenarbeit mit dem/der ISB erarbeitet und muss von der Geschäftsleitung in Kraft gesetzt werden.

Der/Die ISB ist verpflichtet, jede Richtlinie jährlich zu überprüfen und ggf. an die aktuellen Vorschriften (bspw. gesetzliche, vertragliche, behördliche) anzupassen.

Werden Änderungen an einer bestehenden Richtlinie vorgenommen oder wird eine neue Richtlinie erstellt, muss diese zeitnah den betreffenden Stakeholdern/Stakeholderinnen vorgelegt und ggf. verständlich erläutert werden.

Jede geltende Informationssicherheitsrichtlinie ist verpflichtend. Wird eine Richtlinie nicht mehr benötigt, muss diese durch die Geschäftsleitung aufgehoben werden.

Eine Richtlinie muss die folgenden Anforderungen erfüllen:

- Definition der Zielgruppe
  - Für wen ist diese Richtlinie handlungsweisend?
- Grund der Erstellung und Zielsetzung
  - Warum wird diese Richtlinie erstellt und was soll damit bezweckt werden?
- Kein Verstoß gegen die Leitlinien und Richtlinien des Unternehmens
- Kein Verstoß gegen andere Richtlinien, Gesetze oder Verordnungen
- Hinweis auf Nichtbeachtung
  - Was passiert, wenn die Richtlinie nicht eingehalten wird?
- Beschreibung von ggf. vorhandenen Ausnahmen
  - In Einzelfällen kann eine Richtlinie begründete Ausnahmen enthalten. Diese müssen jedoch genehmigt und dokumentiert werden.
- Verweis auf mitgeltende Unterlagen

Ist eine Informationssicherheitsrichtlinie aktiv, so gelten für die Zielgruppe dieser Richtlinie bestimmte Regelungen, die vorher von dem/der ISB festgelegt werden müssen.

Schritt 5.1: ISR – Mitarbeitende

Verantwortlichkeiten:

- Die Geschäftsleitung setzt diese ISR in Kraft und ist für die Einhaltung verantwortlich – kann diese Aufgabe jedoch delegieren.
- Die ISR wird von dem/der ISB in Zusammenarbeit mit dem IST entwickelt.

Ziele:

- Sicherstellung der Aufrechterhaltung der Informationssicherheit durch die Mitarbeitenden.

Aktivität:

- Vor Aufnahme der Tätigkeit von Mitarbeitenden
  - Überprüfung auf Eignung und Vertrauenswürdigkeit
- Bei Aufnahme der Tätigkeit von Mitarbeitenden
  - Schriftliche Erklärung zu Vertraulichkeit
  - Einweisung und Schulung in die Informationssicherheitsleitlinie und alle relevanten Reglungen
  - Freischaltung der erforderlichen IT-Ressourcen, Zugänge und Zugriffsrechte
  - Schulungen in Bezug auf die IT-Ressourcen
- Bei Beendigung oder Wechsel der Tätigkeit von Mitarbeitenden
  - Überprüfung und Anpassung der zur Verfügung gestellten IT-Ressourcen, Zugänge und Zugriffsrechte
  - In Kenntnis setzen aller relevanten Stakeholder/Stakeholderinnen über die Änderung

Erläuterung der Aktivitäten:

Für die Implementierung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems sind die Mitarbeitenden ein zentraler Faktor.

- Vor Aufnahme der Tätigkeit
  - Die angehenden Mitarbeitenden müssen vorab auf die Eignung und die Vertraulichkeit hin überprüft werden.
    Hierfür werden manchmal polizeiliche Führungszeugnisse angefragt.
- Bei Aufnahme der Tätigkeit
  - Die Mitarbeitenden müssen eine Vertraulichkeitsvereinbarung unterzeichnen, die sie zur Verschwiegenheit über unternehmensinterne Informationen verpflichtet. Diese Verschwiegenheitspflicht bleibt auch nach der Beendigung oder der Veränderung des Arbeitsverhältnisses bestehen.
  - Jeder/Jede Mitarbeitende muss bei Aufnahme der Tätigkeit über die Informationssicherheitsleitlinie des Unternehmens unterrichtet und im Umgang mit dieser geschult werden.
  - Für die Dauer des Arbeitsverhältnisses erhält der/die Mitarbeitende nur die im Rahmen seiner Tätigkeit erforderlichen IT-Ressourcen, Zugänge und Zugriffsrechte.
    Beispiele:
    - Ein(e) neue(r) Mitarbeitende(r) bekommt einen **Arbeitsplatz mit Computer** und die Zugangsinformationen und Zugriffsrechte für **Nutzende ohne administrative Rechte**.
    - Die Geschäftsleitung eines Unternehmens hat aufgrund ihrer Stellung hochrangige Zugriffsrechte, sollte aber dennoch nicht mit den administrativen Rechten ausgestattet sein. Dafür ist die Systemadministration zuständig.
  - Alle Mitarbeitenden müssen im Umgang mit den zu nutzenden IT-Ressourcen geschult werden.

    Beispiele:
    - Nur vom Unternehmen freigegebene Speicherorte dürfen für die dauerhafte Speicherung von Daten verwendet werden.
      (bspw. Netzwerklaufwerke)
    - Hard- und Software darf nicht von jedem/jeder Mitarbeitenden eigenmächtig verändert werden. (bspw. Umstecken von Bildschirmkabeln)
    - Netzwerkverbindungen (Zugänge zum Internet, VPN-Verbindungen, …) dürfen nicht eigenmächtig eingerichtet oder verändert werden.

  - Sicherheitsrelevante Einrichtungen und Maßnahmen dürfen nicht eigenmächtig deinstalliert, deaktiviert oder verändert werden.
    (bspw. Kensington-Schlösser, elektronische Schließmechanismen, …)
  - Die Verwendung von trivialen oder leicht zu entschlüsselnden Authentifizierungsmerkmalen ist untersagt.
    (bspw. Passwörter wie „Password“ oder „123456“)

  Über jede Regeländerung oder -erstellung müssen die Mitarbeitenden zeitnah unterrichtet und darin geschult werden.

  Laut der Cybersecurity Studie 2023 sind **55 % der Maßnahmen** nach einem IT-Sicherheitsvorfall **bessere bzw. intensivere** Schulungen der Mitarbeitenden [3, S. 19]!

- Bei Beendigung oder Wechsel der Tätigkeit
  - Bei Beendigung des Arbeitsverhältnisses oder Wechsel der Tätigkeit sind alle zugewiesenen IT-Ressourcen zu überprüfen und ggf. anzupassen.
    - Zugänge sind zu deaktivieren
      - Abgabe der Schlüssel und -karten
      - Abgabe des Unternehmensausweises
    - Zugriffsrechte sind zu entziehen
    - Abgabe von z. B. zur Verfügung gestellten Notebooks oder Tablets
    - Benutzerkonten sind zu löschen
    - gemeinsam genutzte Zugänge müssen neu eingerichtet bzw. die Authentifizierungsmerkmale verändert werden
  - In-Kenntnissetzen aller relevanten Stakeholder/Stakeholderinnen über die Änderung
    - Ein(e) Pförtner(in) sollte bspw. darüber informiert werden, dass ein(e) Mitarbeitende(r) nicht mehr für das Unternehmen arbeitet, damit dieser/diese nicht wie gewohnt das Gelände betreten kann.
  - Hierfür ist es bei einer Beendigung oder einem Wechsel des Beschäftigungsverhältnisses im Einvernehmen üblich, dass ein(e) Mitarbeitende(r) kurz vor Ende einen Laufzettel erhält, der aufzeigt welche Ressourcen er oder sie zurückgeben muss und welche Daten gesichert werden sollten.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 7** oder der **VdS 10005 Kapitel 6** nachgelesen werden.

Schritt 5.2: ISR – Wissen [6]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit den Vertretungen im IST ein Verfahren, um das Wissen in Bezug auf die Informationssicherheit aktuell zu halten, die Mitarbeitenden davon zu unterrichten und zu schulen.
- Die Geschäftsleitung ist dafür zuständig, dieses Verfahren in Kraft zu setzen.

Ziele:

- Das Unternehmen verfügt zu jedem Zeitpunkt über das aktuellste Wissen im Bereich der Informationssicherheit.
- Alle Mitarbeitenden verstehen ihre Verantwortlichkeiten und sind für ihre Tätigkeit geeignet und qualifiziert.

Aktivität:

- Implementierung eines Verfahrens, das bei einer Änderung der rechtlichen und technischen Bedingungen alle relevanten Stellen des Unternehmens und ggf. relevante externe Stellen in geeigneter Weise informiert.
- Implementierung eines Verfahrens zur Sensibilisierung und Schulung der Mitarbeitenden.

[6] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Für das Verfahren zur Mitteilung über geänderte rechtliche und technische Bedingungen muss folgendes gelten:
  - Es müssen regelmäßig aus verlässlichen Quellen Informationen (insb. akute Gefährdungen und mögliche Gegenmaßnahmen) über die technischen und rechtlichen Entwicklungen eingeholt werden.
    Verlässliche Quellen sind hierbei u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt/die Landeskriminalämter (BKA/LKÄ).
  - Die erhaltenen Informationen müssen unternehmensspezifisch ausgewertet und die betroffenen Bereiche ggf. angepasst werden.
  - Relevante Entwicklungen sind dem/der ISB und der Geschäftsleitung zeitnah mitzuteilen.
- Für das Verfahren zur Schulung und Sensibilisierung von Mitarbeitenden muss folgendes gelten:
  - Die Durchführung erfolgt regelmäßig und zusätzlich bei Bedarf.
  - Die Art und das Intervall müssen zielgruppenorientiert festgelegt werden.
  - Durch die Schulungen werden die Mitarbeitenden im Umgang mit den Inhalten der Informationssicherheitsleitlinie, der verschiedenen Informationssicherheitsrichtlinien und anderer relevanter Regelungen gestärkt.
  - In diesen Schulungen werden die Mitarbeitenden über die aktuellen Gefährdungen und das Verhalten bei Störungen, Ausfällen und Sicherheitsvorfällen informiert und dadurch wird die Akzeptanz der Sicherheitsmaßnahmen bei der Belegschaft erhöht.
- Die Teilnahme der Mitarbeitenden sowie die Inhalte der Schulungen sollten dokumentiert werden.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 8** nachgelesen werden.

Schritt 5.3: ISR – Identifizieren kritische IT-Ressourcen [7]

Verantwortlichkeiten:

- Der/Die ISB ist für die Durchführung dieser Informationssicherheitsrichtlinie verantwortlich und verpflichtet, diese jährlich zu überprüfen.
- Die Geschäftsleitung muss diese ISR freigeben.

Ziele:

- Ermittlung und Identifikation der kritischen IT-Ressourcen des Unternehmens

Aktivität:

- Durchführung einer **Informationsklassifizierung** nach ISO/IEC 27001 [12]

  oder

- Durchführung einer **Schutzbedarfsanalyse** gemäß BSI-Standard 200-2 [18]

  oder

- andere Vorgehensweise

Erläuterung der Aktivitäten:

- Bei einer Schutzbedarfsanalyse werden die IT-Systeme, Örtlichkeiten, Anwendungen und Geschäftsprozesse auf ihren Schutzbedarf hin analysiert. Das BSI hat dafür am Beispiel des fiktiven Unternehmens *Recplast* eine Schutzbedarfsanalyse durchgeführt. Eine Schutzbedarfsfeststellung ähnlich der des Unternehmens Recplast sollte auf das eigene Unternehmen adaptiert werden.

Geschäftsprozesse

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf
GP001	Produktion	Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis zur	Hoch Durch die Entwicklung von	Hoch Gefälschte oder falsche	Sehr Hoch Ein Ausfall
GP002	Angebotswesen	In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im	Hoch Es werden	Hoch Fehlerhafte Daten werden	Normal Ein Ausfall
GP003	Auftragsabwicklung	Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Zusätzlich bietet die	Hoch Es werden	Hoch Fehlerhafte oder manipulierte	Hoch Ein Ausfall
GP004	Einkauf	In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den	Hoch Es werden Verträge und	Normal Fehlerhafte Daten werden in	Normal Ein Ausfall
GP005	Disposition	In der Disposition werden alle für die Produktion benötigten Materialien (Kunststoffe, Schrauben,	Normal Es werden keine vertraulichen	Hoch Fehlerhafte Daten können zu	Hoch Ein Ausfall
GP006	Personalverwaltung	In dieser Abteilung werden alle Aufgaben bearbeitet, die zur administrativen Abwicklung	Hoch Es werden	Normal Fehlerhafte Daten können zu	Normal Ein Ausfall

Abbildung 5: Auszug aus der Schutzbedarfsfeststellung des BSI zu Recplast [7]

[7] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Schritt 5.4: ISR – IT-Systeme

Verantwortlichkeiten:

- Der/Die ISB entwickelt diese ISR in Zusammenarbeit mit dem IST.
- Die Geschäftsleitung ist für die Inkraftsetzung dieser ISR verantwortlich.

Ziele:

- Strukturierte Verwaltung der IT-Systeme und deren Absicherung.

Aktivität:

- Inventarisierung
  Implementierung eines Verfahrens zur Inventarisierung aller IT-Systeme im Unternehmen
- Basisschutz
  Jedes IT-System bedarf eines Basisschutzes gemäß **VdS 10000 Kapitel 10.3**.
- Lebenszyklus
  Ein IT-System besteht aus Hard- und Software. Für diese sog. Funktionseinheit müssen Verfahren implementiert werden, die diese Systeme von der Inbetriebnahme bis zur Ausmusterung begleiten.
- Zusätzliche Maßnahmen für mobile IT-Systeme
  Für mobile IT-Systeme im Unternehmensnetzwerk gelten besondere Sicherheitsmaßnahmen, da diese besonders der Gefahr von Diebstahl, unautorisiertem Zugriff oder unsicheren Netzwerken ausgesetzt sind.
  Für sie gelten die Regelungen, die in **Kapitel 10.4 der VdS 10000** beschrieben werden.
- Zusätzliche Maßnahmen für kritische IT-Systeme [8]
  Für alle kritischen IT-Systeme müssen zusätzlich die Regelungen gemäß **Kapitel 10.5 der VdS 10000** umgesetzt werden.

[8] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Inventarisierung

  Jedem IT-System, das inventarisiert wird, muss ein eindeutiges Identifizierungsmerkmal, ein Einsatzzweck und eine Lokalisierungsangabe (in der obigen Analogie: Straße und/oder Hausnummer) zugeordnet werden.

  Darüber hinaus wird empfohlen, dass noch weitere Informationen (Name, Versionen und Lizenzinformationen, installierte Software, Seriennummern, herstellendes Unternehmen, Garantieinformationen, Serviceverträge, …) erfasst werden.

- Basisschutz

  Hierzu zählen u. a. folgende Maßnahmen:

  - Maßnahmen zur Beschaffung von Software
    (z. B. vertrauenswürdige Quellen),
  - Maßnahmen zur Beschränkung des Netzwerkverkehrs
    (bspw. muss nicht jede/r Nutzende Zugriff auf das Archiv haben),
  - Maßnahmen zur Protokollierung von Ereignissen
    (gescheiterte/erfolgreiche Anmeldeversuche, Fehlercodes, sonstige Ereignisse),
  - Maßnahmen zum Schutz vor Schadsoftware u. v. m.
    Hierbei ist darauf zu achten, dass ein produzierender Bereich eines Unternehmens besonders geschützt werden muss, da ein Echtzeit-Schutz während der laufenden Produktion oftmals nicht möglich ist.

  Das Implementieren eines Basisschutzes für ein IT-System umfasst sehr viele einzelne Maßnahmen, deren Beschreibung in diesem Leitfaden zu umfangreich wären und deshalb in der **VdS 10000 Kapitel 10.3** nachgelesen werden können.

- Lebenszyklus

  Es ist für jedes der beiden Stadien eines IT-Systems (Inbetriebnahme/Änderung und Ausmusterung/Wiederverwendung) ein Verfahren zur Überprüfung zu integrieren.

  Inbetriebnahme/Änderung:

  - Ist das IT-System systemkritisch? Ist der Basisschutz umgesetzt?
  - Aktualisierung des Netzwerkplans und der Inventarisierung
  - Dokumentation der Arbeitsschritte

  Ausmusterung/Wiederverwendung

  - Sicherung bzw. Archivierung der Daten
  - Schutz der Daten vor unberechtigtem Zugriff (ggf. Löschung der Daten)
  - Aktualisierung des Netzwerkplans und der Inventarisierung
  - Dokumentation der Arbeitsschritte

- Zusätzliche Maßnahmen für mobile IT-Systeme
  Beispielhafte Maßnahmen sind:

  - Mobile IT-Systeme dürfen bei Verlust oder Beschädigungen keine Informationen an Dritte preisgeben.
  - Vorabdefinition von Verhaltensweisen in Bezug auf das mobile IT-System.

  Es gibt zahlreiche Maßnahmen für mobile IT-Systeme, deren Beschreibung in diesem Leitfaden zu weit gehen würden und deshalb in der **VdS 10000 Kapitel 10.4** nachgelesen werden können.

- Zusätzliche Maßnahmen für kritische IT-Systeme

  - Ein Unternehmen sollte für jedes kritische IT-System ein Notbetriebsniveau implementieren und ein passendes Ersatzsystem verfügbar halten.
  - Regelmäßige Updates sollten vorher auf einem vergleichbaren System getestet werden. Dies ist explizit für den produzierenden Bereich eines Unternehmens wichtig, da eine fehlerhafte Software sehr schnell zu einem Totalausfall im Unternehmen führen kann.
  - Kritische IT-Systeme sollten dauerhaft überwacht werden.

  Es gibt zahlreiche Maßnahmen für kritische IT-Systeme, deren Beschreibung in diesem Leitfaden zu weit gehen würden und deshalb in der **VdS 10000 Kapitel 10.5** nachgelesen werden können.

Genauere Informationen zu dieser ISR sind in der **VdS 10000 Kapitel 10** beschrieben.

Schritt 5.5: ISR – Netzwerke und Verbindungen

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die Inkraftsetzung dieser verantwortlich.

Ziele:

- Abgesicherte Kommunikation über alle Netzwerke (intern und extern) hinweg

Aktivität:

- Netzübergänge sichern
- Implementierung eines Basisschutzes für Netzwerke
- Risikoanalyse für kritische Verbindungen

Erläuterung der Aktivitäten:

- Die Informationssicherheitsrichtlinie muss für jeden Netzübergang zu weniger stark gesicherten Netzwerken angewendet werden.
  - Beschränkung des Netzwerkverkehrs auf das funktionale Minimum
  - Untersuchung und ggf. Blockierung von Schadsoftware
  - Behandlung von Schadsoftware als Sicherheitsvorfall
  - Jährliche Überprüfung der Konfiguration aller Netzwerkkomponenten
- Implementierung eines Basisschutzes für Netzwerke
  - Nicht dauerhaft genutzte Netzwerkanschlüsse müssen vor unberechtigter Nutzung gesichert werden.
  - Prüfung, ob eine Segmentierung des Unternehmensnetzwerkes möglich ist.
  - Absicherung der Daten vor Fernzugriffen (z. B. für Wartung) und bei Netzwerkkopplungen bzgl. der Schutzziele Vertraulichkeit, Integrität und Authentizität (z.B. durch anerkannte Sicherheitsstandards wie VPN, ZTNA, SD-WAN, …)
  - Absicherung des WLAN vor Fernzugriffen durch anerkannte Standards (WPA2, WPA3, …)
- Die Risikoanalyse für die kritischen Netzwerkverbindungen ist nach anerkannten Standards (z. B. BSI Standard 200-3 [14]) auszuführen.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 11** oder der **VdS 10005 Kapitel 8** nachgelesen werden.

Schritt 5.6: ISR – Mobile Datenträger [9]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die Umsetzung und die Inkraftsetzung dieser verantwortlich.

Ziele:

- Sicherer Umgang mit mobilen Datenträgern in Bezug auf die Informationssicherheit

Aktivität:

- Bestimmung der Daten, die auf einem mobilen Datenträger gespeichert werden dürfen
- Information der Mitarbeitenden und Nutzenden über die spezifischen Risiken und Gefahren (Diebstahl, Verlust, Einschleppen von Schadsoftware) im Umgang mit mobilen Datenträgern
- Mobile Datenträger mit Unternehmensdaten sind vertraulich zu behandeln
- Schutz der Daten durch geeignete und anerkannte Verschlüsselungsverfahren
- Risikoanalyse für kritische mobile Datenträger

[9] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Bestimmung der Daten, die auf einem mobilen Datenträger gespeichert werden dürfen
  - Daten, die besonders geschützt werden sollten, weil sie beispielsweise personenbezogene Daten oder besonders schützenswerte Unternehmensgeheimnisse enthalten, sollten nicht auf mobilen Datenträgern gespeichert werden.
  - Sollte dies jedoch notwendig sein, sollten diese Daten verschlüsselt werden, sodass keine dritte Partei bei Diebstahl oder Verlust Zugriff auf diese Daten erhalten kann.
- Information der Mitarbeitenden und Nutzenden über die spezifischen Risiken und Gefahren (Diebstahl, Verlust, Einschleppen von Schadsoftware) im Umgang mit mobilen Datenträgern
  - Arbeits-USB-Sticks, auf denen z. B. eine Präsentation gespeichert wurde und die an einem fremden IT-System angeschlossen war, kann von diesem IT-System Schadsoftware übernommen haben. Es ist unbedingt zu vermeiden, dass solche und andere potentiell infizierte Datenträger Zugang zum Unternehmensnetzwerk erhalten.
  - Sind auf einem mobilen Datenträger z. B. die Mischungsverhältnisse von vom Unternehmen entwickelten Stoffen enthalten, sind diese für die Konkurrenz des eigenen Unternehmens von besonderem Interesse.
- Mobile Datenträger mit Unternehmensdaten sind vertraulich zu behandeln
  - Unternehmensdaten umfassen alle Daten, die einen Rückschluss auf das Unternehmen ermöglichen.
- Schutz der Daten durch geeignete und anerkannte Verschlüsselungsverfahren
- Risikoanalyse [14] für kritische mobile Datenträger

Laut den Befragten der Cybersecurity Studie 2023 birgt die private Nutzung von Firmengeräten erhebliche Gefahren. [3, S. 29]

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 12** nachgelesen werden.

Schritt 5.7: ISR – Umgebung/Umwelteinflüsse

Verantwortlichkeiten:

- Die Geschäftsleitung ist dazu verpflichtet, das Unternehmen gegen negative Umwelteinflüsse abzusichern.

Ziele:

- Schutz von Servern, aktiven Netzwerkkomponenten, Netzwerkverteilstellen und Datenleitungen gegenüber äußeren negativen Einflüssen.

Aktivität:

- Die Entwicklung der ISR sollte mithilfe eines anerkannten Standards (z. B. VdS 2007 [19]) erfolgen.

Erläuterung der Aktivitäten:

- In dem Standard VdS 2007 [19] werden potentielle Gefahren von außerhalb und dazugehörige mögliche Schutzmaßnahmen aufgezeigt. Ebenfalls sind hierin Tabellen enthalten, die eine Schutzbedarfsanalyse mit dazugehörigen Maßnahmen enthalten.
- Eine Möglichkeit, ein Unternehmen zu schützen, zeigt das sog. „Defence in Depths“-Konzept. Bei diesem Konzept wird die Sicherung des Unternehmens ähnlich einer Zwiebel aufgebaut. Jede Zwiebelschicht steht sinnbedeutend für eine Verteidigungslinie (z. B. Firewall) nach außen hin. Die äußerste Schale stellt z. B. ein umgebender Zaun dar. Näher Informationen zu diesem Konzept sind im ersten Bereich der DIN EN IEC 62443 [20] Normenreihe zu finden.
- Da der Standard frei verfügbar ist, wird in diesem Leitfaden auf eine detaillierte Darstellung verzichtet und lediglich auf den Standard verwiesen.

Wird ein anderer Standard als die **VdS 2007** zur Entwicklung der ISR gewählt, so sind die Anforderungen aus **VdS 10000 Kapitel 13** oder aus **VdS 10005 Kapitel 9** zu erfüllen. Genauere Informationen zu dieser ISR können dort ebenfalls nachgelesen werden.

Schritt 5.8: ISR – IT-Outsourcing und Cloud-Computing

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Unternehmensleitung ist für die Inkraftsetzung dieser verantwortlich.
- Die Unternehmensleitung ist zusätzlich für die Einhaltung der Verträge mit externen Dienstleistenden und die Gestaltung der Verträge zuständig.
- Die Administration ist für die technische Umsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Delegation von Verantwortung an externe Unternehmen
- Wahrung der IT-Sicherheitsinteressen des Unternehmens
- Einsparung von materiellen und/oder personellen Ressourcen

Aktivität:

- Jedes Vorhaben, Aspekte der IT des Unternehmens auszulagern, muss dokumentiert werden.
- Das Unternehmen und die Mitarbeitenden müssen über die Auslagerung von IT-Ressourcen informiert und auf diese vorbereitet bzw. im Umgang damit geschult werden.
- Die Verträge müssen so gestaltet werden, dass das anbietende Unternehmen sämtliche Anforderungen bzgl. der IT-Sicherheitsinteressen des eigenen Unternehmens erfüllt.

Erläuterung der Aktivitäten:

- Für jedes Vorhaben, Aspekte der IT des Unternehmens auszulagern, müssen folgende Punkte zwingend dokumentiert werden:
  - Welche IT-Ressourcen werden ausgelagert?
  - Müssen betriebliche, gesetzliche und vertragliche Bestimmungen insbesondere in Bezug auf die drei Hauptschutzziele Vertraulichkeit, Integrität und Verfügbarkeit beachtet werden?
  - Ist die auszulagernde IT-Ressource eine kritische IT-Ressource?
- Das Unternehmen und die Mitarbeitenden müssen über die Auslagerung von IT-Ressourcen informiert und auf diese vorbereitet bzw. im Umgang damit geschult werden.
- Die Verträge müssen so gestaltet werden, dass das anbietende Unternehmen sämtliche Anforderungen bzgl. der IT-Sicherheitsinteressen des eigenen Unternehmens erfüllt.
  - Ansprüche aus Vertragsverletzungen gegen das anbietende Unternehmen können auch durchgesetzt werden, wenn dieses sich nicht im selben Rechtsraum befindet.
  - Bei einer Beendigung des Vertrages (Insolvenz oder Auflösung) wird vereinbart, dass sämtliche IT-Ressourcen in Bezug auf das Unternehmen herausgegeben werden müssen.
  - Weiterhin wird vereinbart, dass bei Beendigung des Vertrages das ehemalige anbietende Unternehmen den Migrationsprozess zum neuen Anbieter unterstützen muss.
  - Einhaltung der Datenschutzbestimmungen gemäß VdS 10010

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 14** oder der **VdS 10005 Kapitel 11** nachgelesen werden.

Schritt 5.9: ISR – Zugänge und Zugriffsrechte [10]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.
- Die Administration ist für die technische Umsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Mithilfe der Zugänge und Zugriffsrechte wird der Zugang zu den internen IT-Ressourcen gewährt. Diese müssen vor unberechtigtem Zugriff geschützt werden.

Aktivität:

- Implementierung von Verfahren zum Anlegen, Ändern und Zurücksetzen von Zugängen und Zugriffsrechten
- Jährliche Überprüfung der Zugänge und Zugriffsrechte zu kritischen IT-Ressourcen.

[10] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Implementierung von Verfahren zum Anlegen, Ändern und Zurücksetzen von Zugängen und Zugriffsrechten
  - Jeder Vorgang muss beantragt, geprüft und von der/dem ISB genehmigt werden.
  - Genehmigungen werden nur erteilt, wenn diese für die Aufgabenerfüllung des/der Nutzenden notwendig sind.
  - Administrative Zugänge und Zugriffsrechte bedürfen besonderen Begründungen.
  - Antragsstellende (meist die Nutzenden) müssen zeitnah über das Anlegen und Ändern informiert werden. Auf die Information beim Löschen kann verzichtet werden.
  - Alle Vorgänge müssen ausführlich dokumentiert werden.
- Jährliche Überprüfung der Zugänge und Zugriffsrechte zu kritischen IT-Ressourcen.
  - Jährliche Erfassung und Überprüfung aller Zugänge und Zugriffsrechte bei kritischen IT-Ressourcen
  - Nicht (mehr) benötigte Zugänge und Zugriffsrechte sind zu entfernen
  - Nicht ordnungsgemäß angelegte Zugänge sind als Sicherheitsvorfall (Schritt 5.12) zu betrachten.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 15** nachgelesen werden.

Schritt 5.10: ISR – Datensicherung und -archivierung

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.
- Die ggf. vorhandene Administration ist für die technische Umsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Absicherung der Verfügbarkeit der Daten durch Datensicherungs- und -archivierungsverfahren, da unbrauchbare oder verlorene Daten nicht entsetzt werden können.

Aktivität:

- Festlegung der Speicherorte
- Archivierung ausgewählter Daten, um betrieblichen, gesetzlichen und vertraglichen Anforderungen zu genügen
- Implementierung von Verfahren zur Datensicherung, -archivierung und -wiederherstellung
- Jährliche Überprüfung der Datensicherungen und Archivierungen
- Implementierung eines Basisschutzes für jeden Speicherort und jedes IT-System
- Besondere Verfahren bei kritischen IT-Systemen
- Implementierung von Wiederanlaufplänen

Erläuterung der Aktivitäten:

- Die Speicherorte sollten unter Zuhilfenahme der **3**-**2**-**1**-Methode gewählt werden. Diese Methode sieht vor, dass **drei** Datenkopien erstellt werden.

  Zwei Datenkopien werden auf verschiedenen Speichermedien und **die dritte Datenkopie** an einem anderen Ort aufbewahrt.

- Viele Daten müssen aufgrund von betrieblichen, gesetzlichen und vertraglichen Auflagen für einen bestimmte Zeitraum zur Verfügung stehen und sollten daher archiviert werden. Der Basisschutz für einen Speicherort kann äquivalent zu dem eines IT-Systems aus Schritt 5.4 aufgebaut werden.
- Die Vorgaben der VdS-Richtlinien hierzu sind sehr umfangreich und übersteigen den Rahmen dieses Leitfadens. Nachzulesen sind alle genannten Punkte in der
  - **VdS 10000 Kapitel 16** für kleine und mittlere Unternehmen

    oder der
  - **VdS 10005 Kapitel 10** für kleine und sehr kleine Unternehmen.

Schritt 5.11: ISR – Störungen und Ausfälle [11]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.
- Die (System-)Administration ist für die technische Instandsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Zügige Rückkehr zum Regelbetrieb und Schadensminimierung nach Störung oder Ausfall

Aktivität:

- Implementierung eines Business Continuity Managements (BCM) nach anerkanntem **BSI Standard 200-4** [21] oder **DIN EN ISO 22301** [22].

[11] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Ein Business Continuity Management ist im Grunde das Notfall- bzw. Krisenmanagement des Unternehmens. Hierbei werden verschiedene Bereiche abgedeckt:
  - IT-/System-Ausfall
  - Gebäudeausfall
  - Ausfall von Dienstleistenden
- Für ein einfaches Notfallmanagement sollten folgende Punkte bedacht werden:
  - Bestimmung eines/r **IT-Notfall-Beauftragten**, der/die im Falle eines Notfalls sofort und zu jedem Zeitpunkt kontaktiert werden kann.
  - Erstellen oder Ausfüllen einer **IT-Notfallkarte** (ähnlich zu den Notfallkarten in einem Flugzeug), damit die Mitarbeitenden informiert sind und wissen, was bei einem Notfall zu tun ist. Diese sollte jedem/jeder Mitarbeitenden in einer offline-Version zur Verfügung stehen.
    Diese Notfallkarte sollte die Erreichbarkeit der/s **IT-Notfall-Beauftragten** sowie das Verhalten während eines Notfalls enthalten.
  - Während des Notfalls sollten alle Sachverhalte genauestens dokumentiert werden.

Abbildung 6: Beispielhafte Notfallkarte [14]

Wird eine andere Vorgehensweise gewählt oder sind genauere Informationen erwünscht, so sind die Anforderungen an diese ISR in der **VdS 10000 Kapitel 17** oder dem **BSI Standard BSI 200-4** [21] nachzulesen.

Schritt 5.12: ISR – Sicherheitsvorfälle [12]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.

Ziele:

- Schnelle Eindämmung und Behebung von Schäden

Aktivität:

- Treffen von Regelungen für den Umgang mit IT-Sicherheitsvorfällen
- Implementierung von Maßnahmen zur Erkennung
- Implementierung eines Verfahrens zur zeitnahen Reaktion

[12] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Treffen von Regelungen für den Umgang mit IT-Sicherheitsvorfällen
  - Definition des Begriffes „Sicherheitsvorfall“.
  - Jedem/r Mitarbeitenden sollte es erlaubt und möglich sein, Sicherheitsvorfälle zu melden (positive Fehlerkultur/anonyme Meldewege).
  - Definition der Art der Kommunikation (auch gegenüber der Geschäftsleitung) über diesen Sicherheitsvorfall.
  - Sicherheitsvorfälle sind von der/dem ISB vorrangig zu bearbeiten.
- Implementierung von Maßnahmen zur Erkennung
  - Implementierung von Angriffserkennungssystemen im Unternehmensnetzwerk (bspw. Prüfsummen zur Integritätsprüfung, sog. Honeypots, usw.)
- Implementierung eines Verfahrens zur zeitnahen Reaktion
  1. Schnelle Übersichtgewinnung und ggfs. Schutz von Personen
  2. Schadenseindämmung und -dokumentation
  3. Beweissicherung
  4. Schadensbehebung & Wiederanlauf
  5. Nachbereitung/Verbesserungen

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 18** nachgelesen werden.

5 Leitfaden zur Einführung eines ISMS bei KMU – Abschluss

Wenn die vorangegangenen Schritte durchgeführt wurden, wurde ein Informationssicherheitsmanagementsystem passend zu dem Unternehmen in den Unternehmensablauf integriert. Ein solches Managementsystem muss jedoch regelmäßig an sich ändernde Regularien und Vorschriften angepasst werden. Hierfür sollten in regelmäßigen Abständen (ungefähr jährlich) die eben getroffenen Entscheidungen und Maßnahmen überprüft und ggf. an die geänderten Rahmenbedingungen angepasst werden.

Wenn größere Änderungen im Unternehmen vorgenommen werden (z. B. Abteilungen eröffnen oder schließen, Standorte eröffnen oder schließen, usw.), kann es erforderlich werden, das ISMS auch vor Ablauf eines Jahres grundlegend anzupassen.

Abschließend ist noch zu erwähnen, dass laut der anfangs erwähnten TÜV-Studie die Ausgaben in Bezug auf die Informationssicherheit in KMU in den letzten zwei Jahren bei etwa der Hälfte der kleinen und bei etwa 2/3 der mittleren Unternehmen gestiegen sind. Der Trend zeigt, dass immer mehr Unternehmen in die Informationssicherheit investieren (Abbildung 7) [2].

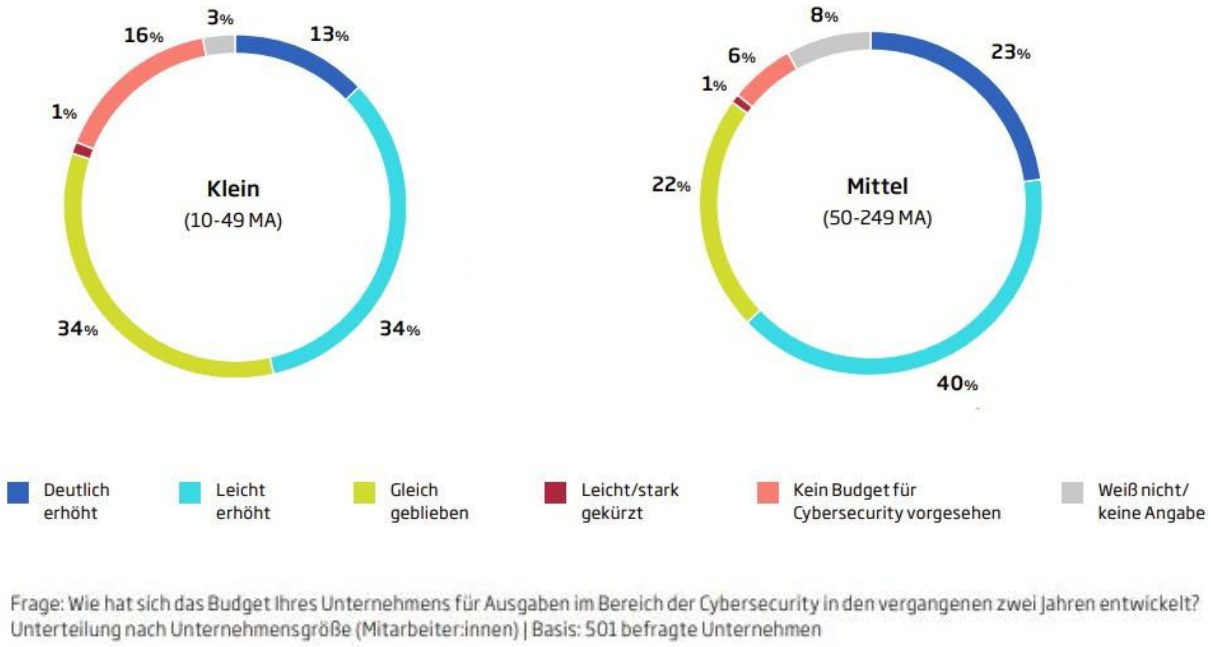

Abbildung 7: Entwicklung der Ausgaben für Cybersecurity [3, S. 34]

Dieser Leitfaden ist ein Instrument, das in den Ablauf des Unternehmens integriert und Teil des Informationssicherheitfortschritts der KMU in Deutschland [3, S. 34] sein sollte. Auch wenn die Kosten für die zusätzlichen Maßnahmen teilweise hoch sein mögen, sagen etwa ⅔ der Unternehmen, dass das Verhältnis zwischen eingesetzten Ressourcen und dem Sicherheitsgewinn ausgeglichen ist [3, S. 39].

6 Abbildungsverzeichnis

7 Abkürzungsverzeichnis/Glossar

Deutsch	Beschreibung
Bedrohung	Durch Schwachstellen ausgelöste potentielle Gefahren werden als Bedrohung angesehen. Wird z.B. der Informationsgehalt einer Nachricht ausspioniert („Man-In-The-Middle“ – Angriff) oder manipuliert, handelt es sich um eine Bedrohung für die beiden Kommunikationspartner. Bedrohungen können darüber hinaus von der Technik (z.B. Kabelbrand), durch eine Fehlbedienung eines Mitarbeitenden (z.B. Überfahren eines Stop-Signals) oder durch das Anwenden von Gewalt ausgehen.
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
Cyberangriff	Von außen (durch einen einzelnen Hacker, durch eine Institution o. ä.) zum Zweck der Sabotage oder der Informationsgewinnung geführter Angriff auf ein Computernetzwerk [23]
DIN	**D**eutsches **I**nstitut für **N**ormung
EN	**E**uropäische **N**orm
Echtzeitschutz	Ein Echtzeitschutz überwacht das System permanent in Echtzeit und schützt jederzeit zuverlässig vor Infektionen. Er läuft automatisch im Hintergrund und überwacht das System kontinuierlich vgl. [24].
IEC	Internationale Elektrotechnische Kommission (**I**nternational **E**lectrotechnical **C**ommission)
ISO	Internationale Organisation für Normung (**I**nternational **O**rganization for **S**tandardization)
KMU	**K**leine (und sehr kleine) und **m**ittlere **U**nternehmen mit weniger als 250 Mitarbeitenden [25] • **sehr kleine** Unternehmen: weniger als **zehn** Mitarbeitende maximale Jahresbilanzsumme von **zwei** Mio. Euro

	• **kleine** Unternehmen: weniger als **50** Mitarbeitende maximale Jahresbilanzsumme von **zehn** Mio. Euro • **mittlere** Unternehmen: weniger als **250** Mitarbeitende maximale Jahresbilanzsumme von **43** Millionen Euro
KRITIS	Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. [26] (Bspw. Klärwerke, Energieversorger, Atomkraftwerke, Chemiekonzerne)
Leitfaden	Kurze, übersichtliche und gut verständliche Handlungsanweisung mit einem leicht bindenden Charakter [27]
Geschäftsleitung	• Oberste Leitungsebene in einem Unternehmen • geschäftsführende Direktion • Inhaber(in) oder Geschäftsführung bei kleineren Unternehmen
Man-In-The-Middle - Angriff	Bei einem „Man-in-the-Middle“-Angriff schaltet sich eine fremde Partei in eine bestehende Kommunikation ein, hört diese – meist unbemerkt – ab und ist in der Lage die Daten zu manipulieren. [28]
Norm	Dokument, das Regeln, Leitlinien oder Merkmale für Tätigkeiten festlegt [29]
Richtlinie	Eine Richtlinie ist eine Handlungs- oder Ausführungsvorschrift einer Institution oder Instanz, die jedoch kein förmliches Gesetz ist. [30]
Risiko	Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit und Ausmaß eines Schadens. Als Risiko werden Szenarien beschrieben, die eine Relevanz für den vorliegenden Fall darstellen [31, S. 33]. Risiken sind das Zusammenspiel aus Assets, Schwachstellen und daraus resultierenden Bedrohungen.

Schwachstelle	Eine Schwachstelle ist eine Lücke in der Informationssicherheit. Sie stellt eine Bedrohung dar, da hierdurch Unbefugten der Zugang zu Systemressourcen und vertraulichen Daten möglich ist. Die Ursachen für die Schwachstelle können in der Konzeption, der verwendeten Algorithmen, der Implementation, der Konfiguration oder dem Betrieb sowie dem Unternehmen liegen [31, S. 33].

Stakeholder/ Stakeholderinnen	Gruppe von Personen, die ein berechtigtes Interesse an der Entwicklung eines Unternehmens haben [32]
	• interne Stakeholder/Stakeholderinnen
	  ○ Mitarbeitende
	  ○ Manager/Managerinnen
	  ○ Eigentümer/Eigentümerinnen
	• externe Stakeholder/Stakeholderinnen
	  ○ Lieferanten/Lieferantinnen
	  ○ Kunden/Kundinnen
	  ○ Gläubiger/Gläubigerinnen

VdS	Ehemals „**V**erband **d**er **S**achversicherer“, heute 100%ige Tochter der „Deutschen Versicherungswirtschaft“ (GDV) [33]
VPN	**V**irtual **P**rivate **N**etwork
ZTNA	**Z**ero **T**rust **N**etwork **A**ccess (Alternative zum VPN) [34]
SD-WAN	**S**oftware-**D**efined – **W**ide **A**rea **N**etwork [35]
WPA2/WPA3	Wi-Fi Protected Access 2/3

8 Literatur

[1] ZDNet-Redaktion. „Jedes 10. Unternehmen Opfer eines Hackerangriffs: Cybersecurity-Studie TÜV-Verband: Phishing und Erpressungssoftware häufigste Angriffsmethoden / Cyber Resilience Act zügig verabschieden." https://www.zdnet.de/88409783/1-von-10-unternehmen-im-jahr-2022-opfer-eines-hackerangriffs/ (Zugriff am: 18. Juni 2023).

[2] Maurice Shahd. „TÜV Cybersecuritystudie 2023." https://www.tuev-verband.de/studien/cybersicherheit-in-deutschen-unternehmen (Zugriff am: 18. Juni 2023).

[3] Dr. Johannes Bussmann, Dr. Gerhard Schabhüser. „Cybersicherheit in deutschen Unternehmen: TÜV Cybersecurity Studie 2023." https://www.tuev-verband.de/?tx_epxelo_file[id]=925194&cHash=11772152e3b993dd496a49e3e533076f (Zugriff am: 18. Juni 2023).

[4] ISACA Germany Chapter e.V. „Implementierungsleitfaden ISO/IEC 27001:2013: Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013." https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf (Zugriff am: 18. Juni 2023).

[5] WissenHoch2, *Cybercrime: Wie können wir uns schützen?* Zugriff am: 15. Juni 2023. [Online]. Verfügbar unter: https://www.3sat.de/wissen/wissenschaftsdoku/230615-sendung-cybercrime-wido-100.html

[6] *VdS 10000 - Informationssicherheits-Managementsystem für kleine und mittlere Unternehmen (KMU),* VdS Schadenverhütung GmbH.

[7] *VdS 10005 - Mindestanforderungen an die IT-Sicherheit für Klein- und Kleinstunternehmen,* VdS Schadenverhütung GmbH.

[8] *DIN SPEC 27076:2023-05, IT-Sicherheitsberatung für Klein- und Kleinstunternehmen,* DIN, Berlin.

[9] Europäische Kommission, *https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act*, 2023. Zugriff am: 19. Juli 2023. [Online]. Verfügbar unter: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[10] Bundesamt für Sicherheit in der Informationstechnik. „Informationen zur Wahl des Geltungsbereiches." https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/Wahl-des-Geltungsbereiches/wahl-des-geltungsbereiches_node.html (Zugriff am: 18. Juni 2023).

[11] *DIN ISO 31000:2018-10, Risikomanagement_ - Leitlinien (ISO_31000:2018),* DIN, Berlin.

[12] *DIN EN ISO/IEC 27001:2017-06, Informationstechnik_ - Sicherheitsverfahren_ - Informationssicherheitsmanagementsysteme_ - Anforderungen (ISO/IEC_27001:2013 einschließlich Cor_1:2014 und Cor_2:2015); Deutsche Fassung EN_ISO/IEC_27001:2017,* DIN, Berlin.

[13] Bundesamt für Sicherheit in der Informationstechnik. „Arbeitsbeispiel RECPLAST GmbH." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/

Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/Recplast.html (Zugriff am: 18. Juni 2023).

[14] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-3 - Risikomanagement." https://www.bsi.bund.de/dok/10027822 (Zugriff am: 18. Juni 2023).

[15] *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung*, DIN EN IEC 62443-3-2:2021-12, DIN, Dez. 2021. [Online]. Verfügbar unter: https://www.beuth.de/de/norm/din-en-iec-62443-3-2/344299957

[16] Europäische Kommission. „Gelten die Vorschriften für KMU?: Datenschutz-Grundverordnung bei KMU." https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_de (Zugriff am: 19. Juli 2023).

[17] Marian Thöne, *Organigramm eines Informationssicherheitsteams: - Eigene Entwicklung eines Schaubildes*, 2023.

[18] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-2 - IT-Grundschutz-Methodik." https://www.bsi.bund.de/dok/10027846 (Zugriff am: 18. Juni 2023).

[19] *VdS 2007 : 2016-03 - Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen,* VdS Schadenverhütung GmbH.

[20] *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber*, IEC 62443-2-1, DIN, Sep. 2020. [Online]. Verfügbar unter: https://www.beuth.de/de/norm-entwurf/din-en-iec-62443-2-1/327919389

[21] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-4 - Business Continuity Management: Community Draft." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (Zugriff am: 18. Juni 2023).

[22] *DIN EN ISO 22301:2020-06, Sicherheit und Resilienz_- Business Continuity Management System_- Anforderungen (ISO_22301:2019); Deutsche Fassung EN_ISO_22301:2019,* DIN, Berlin.

[23] DUDEN. „Cy-ber-at-ta-cke, die." https://www.duden.de/rechtschreibung/Cyberattacke (Zugriff am: 19. Juni 2023).

[24] Avira. „Was ist der Unterschied zwischen Echtzeitschutz und System-Scanner?" https://support.avira.com/hc/de/articles/360000153538-Was-ist-der-Unterschied-zwischen-Echtzeitschutz-und-System-Scanner- (Zugriff am: 20. Juni 2023).

[25] Europäische Kommission, *Definition der Kleinstunternehmen sowie der kleinen und mittleren Un-ternehmen.* Zugriff am: 22. Februar 2023. [Online]. Verfügbar unter: http://data.europa.eu/eli/reco/2003/361/oj

[26] Bundesamt für Sicherheit in der Informationstechnik. „Was sind Kritische Infrastrukturen?: Definition KRITIS." https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-

Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (Zugriff am: 19. Juni 2023).

[27] Dipl. Päd. Uta Reimann-Höhn. „Einen Leitfaden erstellen - Erklärung und Beispiele." https://reimann-hoehn.de/der-leitfaden-erklaerung-und-beispiel/ (Zugriff am: 18. Juni 2023).

[28] Bundesamt für Sicherheit in der Informationstechnik. „Man-In-The-Middle-Angriff." https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html

[29] Stephan Baumann. „Definition Normen - Standards: Normen." https://www.ihk.de/koblenz/unternehmensservice/innovation-und-technologieberatung/normung-und-normen/definition-normen-standards-3325396 (Zugriff am: 19. Juni 2023).

[30] RWB Rechtswörterbuch. „Verfassungsrecht: Richtlinie." https://www.rechtswoerterbuch.de/recht/r/richtlinien/ (Zugriff am: 19. Juni 2023).

[31] Prof. Dr.-Ing. Karl-Heinz Niemann, *IT-Sicherheit in Produktionsanlagen: Vorlesungsskript zur Vorlesung.* Zugriff am: 18. Juni 2023.

[32] BWLWissen.net. „Stakeholder." https://bwl-wissen.net/definition/stakeholder (Zugriff am: 19. Juni 2023).

[33] Baunetz_Wissen. „Glossar: VdS." https://www.baunetzwissen.de/glossar/v/vds-50339 (Zugriff am: 15. April 2023).

[34] Dipl.-Ing. (FH) Stefan Luber / Peter Schmitz. „Was ist Zero Trust Network Access (ZTNA)?: Definition Zero Trust Network Access (ZTNA)." https://www.security-insider.de/was-ist-zero-trust-network-access-ztna-a-959927/ (Zugriff am: 26. Juni 2023).

[35] IBM. „SD-WAN erklärt - Was ist Software-Defined WAN (SD-WAN)?" https://www.ibm.com/de-de/services/network/sd-wan

B. Aufgabenstellung der Bachelorarbeit

Aufgabenstellung aus
Datenschutzgründen entfernt.